NUREG-0653

Report on Nuclear Industry Quality Assurance Procedures for Safety Analysis Computer Code Development and Use

Manuscript Completed: July 1980
Date Published: August 1980

B. W. Sheron, Z. R Rosztoczy

Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

8009100407

ABSTRACT

As a result of a request from Commissioner V. Gilinsky to investigate in detail the causes of an error discovered in a vendor Emergency Core Cooling System (ECCS) computer code in March, 1978, the staff undertook an extensive investigation of the vendor quality assurance practices applied to safety analysis computer code development and use. This investigation included inspections of code development and use practices of the four major Light Water Reactor Nuclear Steam Supply System vendors and a major reload fuel supplier.

The conclusion reached by the staff as a result of the investigation is that vendor practices for code development and use are basically sound.

A number of areas were identified, however, where improvements to existing vendor procedures should be made. In addition, the investigation also addressed the quality assurance (QA) review and inspection process for computer codes and identified areas for improvement.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

APPENDICES

LIST OF FIGURES

LIST OF TABLES

PREFACE

This report, originally scheduled for issuance in April, 1979, was delayed approximately one year due to temporary assignment of the authors to the Bulletins and Orders Task Force in NRR in response to the accident at Three Mile Island-2.

ACKNOWLEDGEMENT

The authors would like to acknowledge Mr. Richard Brickley and Dr. Donald Anderson of the Region IV Office of Inspection and Enforcement who conducted the inspections. Also acknowledged are:

Paul Norian	NRR/DSS/AB
Wayne Hodges	NRR/DSS/AB
Jack Guttmann	NRR/DSS/AB
Rene Audette	NRR/DSS/AB
Norm Lauben	NRR/DSS/AB
John Gilray	NRR/DPM/QAB
Jack Spraul	NRR/DPM/QAB

who participated in the inspections. The total effort expended in this investigation was less than one man-year.

1.0 Introduction

This report documents the results of a staff review of the nuclear industry quality assurance requirements for computer code development and control. This review was conducted by the Analysis Branch, Division of Systems Safety, Office of Nuclear Reactor Regulation, and focuses primarily on Thermal-Hydraulic Safety Analysis computer codes. The review was limited to the four major Nuclear Steam Supply System (NSSS) vendors and one reload fuel supplier. While the review did not include other types of computer codes (e.g., stress analysis) the conclusions reached are considered generally applicable to all aspects of NSS vendor and fuel reload supplier safety analysis code development and control. The applicability of the conclusions to other types of safety analysis code users in the nuclear industry (e.g., architect engineers and applicants) is not established in this report. This report was prepared in response to a request by Commissioner Gilinsky to investigate in detail the cause of a computer code error of the type discovered by Westinghouse in its emergency core cooling system (ECCS) computer code LOCTA.

The report is organized in three major parts. The first part, comprising sections 2 through 4, provides background information regarding the purpose of the review. The second part, sections 5 through 7, describes code development experience, industry practices, and applicable NRC requirements. The third part, sections 8 through 10, presents the staff observations, conclusions and recommendations.

2.0 Summary and Conclusions

The investigation indicates that the nuclear industry quality assurance procedures for safety analysis computer code development and use are basically sound.

The investigation identified a number of areas which should be improved. The more significant conclusions and recommendations are provided below. These conclusions and recommendations, although specifically developed from our investigation of thermal-hydraulic safety analysis code development and use, are considered generally applicable to the development and use of all safety analysis codes.

A. 10 CFR Part 50, Appendix B and Regulatory Guide 1.64, which endorses ANSI N45.2.11-1974, "Quality Assurance Requirements for the Design of Nuclear Power Plants" are considered acceptable controls for the development and use of computer codes. The vendors have developed procedures to comply with these requirements and we found that these procedures, when properly executed, are acceptable. The execution of the procedures did not measure up to staff expectation however, and some of the procedures as well as execution of the procedures were found to need improvement.

Recommendations:

(1) Maintain the present methods of quality assurance.

(2) NRC should assure that the shortcomings found in the procedures are promptly corrected.

(3) NRC should audit the execution of the procedures for computer code development and use more often, using a multidiscipline team for the audit. (See Item D below)

B. In addition to ANSI N45.2.11-1974 endorsed by NRC, there are two additional ANSI standards presently available which pertain to quality assurance for computer code development and use. These standards have not been endorsed by NRC however.

Recommendation:

(4) NRC should review ANSI-N413, "Guidelines for the Documentation of Computer Programs" and ANSI/ANS-10.5-1979, "Guidelines for Considering User Needs in Program Development." If found useful and acceptable, these standards should be officially endorsed by NRC through issuance of a Regulatory Guide.

C. Only the reactor vendors and one fuel supplier were audited during this investigation. There are indications that other segments of the industry (utility companies and Architect-Engineers), the national laboratories, and the NRC might not have quality assurance procedures developed to the same extent as reactor vendors.

Recommendations:

(5) Architect engineering firms and selected utility companies should be audited.

(6) National laboratories which develop and/or use computer programs for safety analyses under contract to the NRC should be audited in the same way as reactor vendors.

(7) NRC should set up internal quality assurance procedures for its audit calculations.

D. Although the examples selected for this special, in-depth investigation were all from the thermal-hydraulic area, we believe the findings are general and are equally applicable to all computer code quality assurance procedures.

Recommendation:

(8) The inspection program recommended under Item E should be adapted for all engineering disciplines.

E. The present version of quality assurance procedures considered applicable to code development and use is relatively new. The NRC vendor inspection program administered by Region IV played an important role in the establishment and development of these procedures. However, we found that the present inspection program is not entirely suited for rendering a judgement on the extent and completeness to which vendors implement code development and verification procedures.

Recommendations:

(9) Region IV should periodically conduct code development and use audits with the help of NRR.

(10) An inspection of the code files should be conducted prior to approval of a given code. The NRR reviewers should participate in the inspection.

F. Some reactor vendors expressed a view that NRC audit calcualtions provided independent verification of their calculations. While NRC may, on occasion, independently check certain vendor analyses, NRC analyses do not provide the independent verification required by the quality assurance procedures. This is the responsibility of the vendors, and under no circumstances should staff audit calculations be relied upon as independent verification of vendor analyses. Generic submittals do not require an affadavit attesting to the correctness of the information submitted as licensing applications do.

Recommendations:

(11) Vendors and applicants (or licensees) should be reminded that they are fully responsible for the quality of their calculations.

(12) Generic submittals, such as code descriptions and engineering calculations should be accompanied by an affidavit as required for licensing applications.

G. There is an apparent problem in the reporting requirements. Vendors are required to report potential safety concerns based on their contractual requirements - in some instances based on 10 CFR Part 21, "Reporting of Defects and Noncompliance." However, an organization currently is not limited in the amount of time they may use to study the issue prior to making a finding regarding the existance of a potential safety concern. The study process often takes months or years.

Recommendation:

(13) Specific time limits should be established to determine if a potential safety concern is reportable when one is filed in the vendor's organization. Alternatively, reporting requirements to NRC of potential safety concerns when they are filed in vendor organizations might also be considered.

H. Vendors have no reporting requirement for code errors which are not covered by contractual requirements. The director or responsible officer of a vendor may have some enforceable regulatory requirements under 10 CFR Part 21 for reporting of code errors. The nature of safety analysis code errors with respect to the reporting requirements in many instances would not require applicants or licensees to report errors.

Recommendations:

(14) Specific criteria for the reporting of computer code errors should be established.

3.0 Background

On March 23, 1978, Westinghouse informed the NRC staff that it had discovered an error in the LOCTA program used to calculate peak cladding temperatures in their ECCS evaluation model. This error involved the zirconium-water heat generation term in the cladding being erroneously decreased by a factor of 2 at the cladding surfaces.

The staff made a preliminary determination of the impact of the error on operating plants and interim penalties on allowable peaking factors were applied. For plants in the licensing process, recalculations by Westinghouse were made on an expedited basis with only the correction made to the code in order to show compliance with the regulations. The long-term resolution involved a submittal by Westinghouse of additional code improvements to offset the effect of the error. Subsequent to approval of the code modifications, Westinghouse recalculated new allowable peaking factors for all affected operating plants.

The discovery of the Westinghouse error was not unique, in that other vendors had previously reported errors in their ECCS evaluation models. (see section 4.0).

The staff decided that a review and inspection of the major vendor and fuel supplier safety analysis code quality assurance requirements would best address Commission and staff concerns.

4.0 Description of Review

The review and inspection of the vendors' thermal-hydraulic safety analysis code quality assurance requirements had three main purposes. The first was to evaluate if sufficient guidelines for quality assurance requirements of safety analysis codes have been developed by NRC. The second was to allow the staff to examine the vendors' existing procedures, and determine if they were adequate to minimize the potential for errors to go undetected in thermal-hydraulic safety analyses. The third was to determine if the vendors were actually following the procedures.

The major elements of this effort were:

(1) Evaluation of existing NRC regulations, regulatory guides and acceptance criteria in Standard Review Plans to determine if sufficient QA control requirements exist for the development and use of computer codes.

(2) Review of of documents relating to the quality assurance of vendor safety analysis computer codes.

(3) Meetings with the vendors to review their computer code quality assurance procedures.

(4) Inspection of vendor records to determine compliance with established quality control procedures.

(5) Evaluation of the findings and derivation of conclusions and recommendations.

Elements 2 and 3 were performed primarily to familiarize the Office of Nuclear Reactor Regulation (NRR) staff with the present procedures being implemented in the vendor organizations. The inspections referred to in element 4 were carried out by the Vendor Inspection Branch of the Region IV Office of Inspection and Enforcement (IE) with NRR assistance.

4.1 Organizational Interactions

Figure 4.1 shows how NRR and IE interact with the vendor organizations as part of the code development process. The basic interactions are as follows:

(1) The Quality Assurance Branch, NRR, is responsible for reviewing, evaluating, and accepting each vendor's Quality Assurance Program description (normally a topical report).

(2) Each vendor is required to establish a set of procedures which satisfy the commitments of the quality assurance program description and any additional standards or guides.

(3) Once the code has been developed, it is submitted to NRR for review and approval (in the case of thermal-hydraulic safety analysis codes, the review is performed by the Analysis Branch).*

(4) At this stage, the code is sometimes used to perform safety analyses.

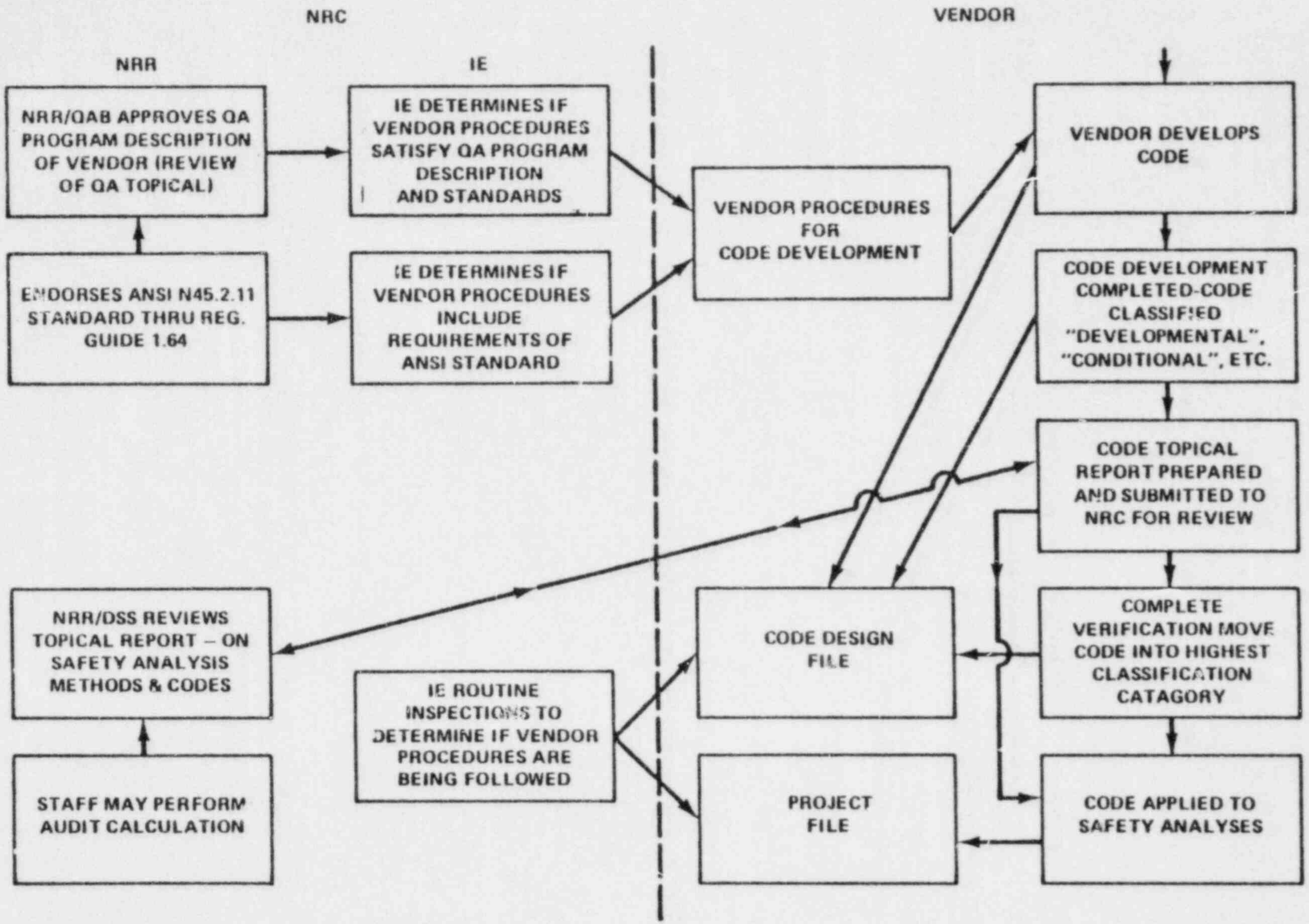
(5) During the development of the code, any information generated is placed in the development file established for that code. Once the development file is at the appropriate stage, the code is certified by the vendor for use.

(6) Certified codes are used for plant safety evaluations. Information developed for the safety evaluation (e.g., input data) is contained in the project file.

(7) At any stage during the development and use of the code, the Vendor Inspection Branch of IE Region IV can inspect the code files and/or the project files.

*Unlike licensing submittals by utility applicants, computer code descriptions are usually submitted as generic topical reports by the vendor, and are not accompanied by an affadavit attesting to the correctness of the submitted information.

FIGURE 4.1
CODE DEVELOPMENT ORGANIZATIONAL RELATIONSHIPS



4.2 Staff Audit Function

Staff audit calculations are part of a staff methods review of a vendor's computer code. They consist of analyses performed by the staff (or their contractors) using computer codes independently developed for staff use, and are intended to duplicate analyses performed by the vendors' computer code. Audit calculations are usually performed whenever a new code is submitted for approval, an existing code has been significantly modified and the modifications are submitted for approval, or there is some other reason to independently audit a vendor's model (e.g., a significant change in plant design). In addition, audit calculations on individual plants are performed if requested by other branches within NRR, such as Reactor Systems Branch, Containment Systems Branch, etc., to assist them in determining design acceptability.

In the case of thermal-hydraulic safety analysis codes, the audit function is performed by the Analysis Branch in the NRR Division of Systems Safety.

The five LWR vendors reviewed in this study use a total of 19 computer codes to calculate the course and consequences of a Loss-of-Coolant Accident (this does not include codes related to fuel performance, containment analysis, subcooled loads analysis, etc.). These 19 codes have been submitted to the NRC and approved by the NRC staff. On the other hand, for analyses of reactor transients other than LOCA, there are approximately 30 codes used by the same five suppliers. Of these, 13 have been approved by the NRC staff. The remainder are still under review.

Because of the different calculational methods used by the vendors and NRC, and because of the complexity of performing accident analyses, differences in results between vendor and NRC calculations are expected. Typically, these differences overshadow the effects of small errors that might exist in either the NRC or a vendor's code. Therefore, audit calculations for thermal-hydraulic safety analyses are only expected to discover large errors.

If any significant discrepancies in the results are seen, the staff will try to resolve the discrepancies with the vendor, and determine if an error is the cause of the discrepancy.

In the past, the staff has found errors in vendor models through the use of audit calculations. In 1974, a staff audit calculations with the TOODEE code uncovered the use of an inappropriate initial cladding oxide thickness in a code used by one of the vendors. This same audit calculation also uncovered an error in the heat transfer coefficients. In 1975, during the review of a vendor's transient code used to analyze anticipated transients without scram (ATWS), the staff suspected that the omission of certain terms in the constitutive equations was producing incorrect results. A follow-up audit calculation using the RELAP3B code confirmed the error and the vendor was required to correct the model.

In areas where the staff has not performed audit calculations, some errors have existed and gone undetected for long periods of time. A recent example of this is the REDY code errors discovered as a result of disagreement between predictions and the results of tests performed in the Peach Bottom reactor. (See item (4) of enclosure (1) to GE trip report in Appendix A.)

4.3 Inspections
4.3.1 Vendor Inspections

The determination that vendors are properly implementing their quality assurance procedures is the responsibility of the Office of Inspection and Enforcement (IE). The Region IV office of IE has the responsibility of performing the vendor inspection program. This program is designed to (1) determine if the vendors are following their procedures, and (2) determine if the vendors' procedures fulfill the commitments of their approved quality assurance program. The inspections by Region IV include NSSS suppliers, fuel reload suppliers, architect engineers, and both ASME* Code and non-code vendors (e.g., valves, valve movers, electrical components). However, if a utility performs its own architect-engineering function, then the applicable region Inspection and Enforcement Office performs the QA inspections.

The scope of IE regional office inspections of applicants was not investigated for this report.

It was observed that the broad range of subjects that must be inspected by Region IV inspectors limits the inspector's capability to properly assess the technical adequacy of the information provided by the vendors in support of both adequacy of the procedures and procedure compliance. In many instances, an inspector must rely on information which supports compliance with administrative aspects of the procedures in order to conclude the technical aspects of compliance are also met.

For example, in the case of computer code development and control QA procedures, the procedures call for a computer code to be verified. What the inspectors examine is whether information exists in the code file pertaining to verification, and that proper documentation that the code was verified in accordance with procedural requirements also exists.

An in-depth review of the documentation of the verification methods used, their applicability to the specific computer code in question, etc., is not performed by the inspectors.

It was also noted that Region IV had not yet developed inspection procedures for auditing code development and control. Inspection procedures are typically used by the inspectors to aid them in inspecting diverse engineering disciplines and to provide an orderly approach to the inspection process. It was felt that development of inspection procedures for code development and use would greatly aid the inspectors in this area. In addition, the multi-discipline team approach used for these inspections worked very well in that the NRR personnel provided technical support to the inspectors in conducting their inspections, and the inspectors helped the NRR technical staff in finding proper information to be examined.

*American Society of Mechanical Engineers

4.3.2 Code Quality Assurance Inspections

The purpose of the vendor inspections performed for this task was not only to provide an assessment of whether vendors were following their procedures and if their procedures fulfill the commitments of their approved quality assurance program, but to answer the following questions (with regard to thermal-hydraulic code development):

(1) Are the design control procedures being appropriately interpreted for code development?

(2) Were previously discovered errors the result of deficiencies in the Quality Assurance procedures and could the errors have been avoided with better procedures?

(3) Are there any critical areas in the code development process in which procedures presently do not exist and are needed?

4.3.3 Scope of Code Quality Assurance Inspections

The vendor quality assurance requirements are applicable to computer code development in general, and not to any one particular type of computer code. Since this review was conducted by the Analysis Branch in the Division of Systems Safety, NRR, it was restricted to those codes within the branch's cognizance, namely thermal-hydraulic codes for analyses of reactor transients and ECCS safety analysis codes. The codes inspected at each organization are listed in Table 4.1. In addition to inspecting code files, the NRC staff examined example project calculational files at some vendor organizations. The causes of some previously reported code errors were also examined. These are listed in Table 4.2. A detailed discussion of these errors can be found in the trip reports of Appendix A. A more precise discussion on what is meant by an "error" is given in section 5.0.

5.0 Code Errors

Code errors can be divided into two types. The first type involves mathematical expressions, parameter values, input data, etc., not existing in the code or being used in an unintentional manner. The second type, code modeling discrepancies, involves the inability of a code (and/or individual models within a code) to predict new experimental data. These types are not considered "errors" in the context of this report, since they neither occur in the same way as the first type of errors do (i.e., unintentionally in the code) nor are they treated by NRC in the same way the first type of errors are. Recent examples of this type are those revealed by the results of the Peach Bottom BWR transient tests and the TLTA (Two-Loop Test Apparatus) tests 6405 and 6007.

5.1 Code Discrepancies

NRC, in many cases, continues to evaluate thermal-hydraulic safety analysis codes subsequent to their approval for use. The Semiscale, LOFT, and TLTA

TABLE 4.1

CODE DEVELOPMENT AND USE FILES AUDITED

ORGANIZATION	ECCS	THERMAL-HYDRAULIC TRANSIENT
Babcock & Wilcox	———	TRAP (STEAM-LINE BREAK)
Combustion Engineering	STRIKIN-II	CESEC (TRANSIENTS)
Exxon Nuclear Corp.	RELAP	PTS-BWR (BWR TRANSIENTS)
Westinghouse	LOCTA (HOT PIN HEATUP)	LOFTRAN (TRANSIENT)
General Electric	· CHASTE (HOT PIN HEATUP) · REFLOOD (REFLOOD HYDRAULICS)	———

TABLE 4.2

PREVIOUS CODE ERRORS AND MODEL DISCREPANCIES EXAMINED*

VENDOR	ERROR	TYPE**	APPARENT CAUSE
B&W	Did not analyze most limiting small break	E	Break size to area relationship not thoroughly examined
B&W	Sign error in gravity head term of CRAFT2 code	E	No line-by-line checking when code was developed
B&W	Steamline break results more severe with new code. Did not fill out PSC (preliminary safety concern)	E	New code considered conservative but degree of conservatism was not quantified
GE	Error in reflood vapor venting	E	Code was not given a detailed design review when it was developed
GE	Core pressure drop for leakage flow	D	Model was not properly verified against applicable data
GE	Use of wrong system pressure during reflood	E	Review are only done on individual codes, not overall analytical methods
GE	REDY errors indicated by Peach Bottom Test	D	Model was not properly verified against applicable data
W	Zirconium-water Reaction Rate	E	Insufficient review at time of code development
W	Upper Head Temperature Error	D	Model was not properly verified against applicable data

* The errors identified do not represent all of the errors reported to date, but were selected as examples for the purposes of this review.

** E-Error; D-Model Discrepancy

TABLE 4.2 (continued)

VENDOR	ERROR	TYPE**	APPARENT CAUSE
W	Total steam flow calculation did not include safety valve flow	E	Incomplete checking of computer input card deck
CE	Numerous programming errors	E	No line-by-line checking when code was developed
ENC	None reported to date	—	—

programs have been and continue to be used extensively for this purpose in the area of LOCA analysis verification.

Through the Standard Problem Program, industry and international participants evaluate the capabilities of their LOCA codes to predict selected experimental data from these and other facilities. Infrequently, a discrepancy may be seen between the expected or predicted system behavior and the actual behavior. Sometimes these discrepancies are due to atypicalities in the experimental facility or test conditions, but in other cases these discrepancies can be traced back to incorrect models in the codes.

Some recent examples of code discrepancies are TLTA tests 6405 and 6007, Peach Bottom BWR Turbine Trip tests, Semiscale test S-07-6, and LOFT test L2-2. The effects of these tests are presently being evaluated.

5.2 Previous Code Errors

The reporting by Westinghouse of the metal-water reaction rate error found in March, 1978, was not unique for ECCS codes. (In contrast to ECCS codes, most errors in non-ECCS codes are not reported to NRC). Since 1974, when the majority of the ECCS models were approved, 4 of the 5 vendors inspected have reported errors. (Detailed discussions of the causes of some previously reported code errors are provided in the staff inspection trip reports in Appendix A to this report.)

These errors were detected in a variety of ways which are generalized as follows:

- Users of the code(s) other than the originators observed anomalous results which were traced to an error.
- Users of the code(s) within the originating organization observed anomalous results which were traced to an error.
- Internal technical audits of codes by the originating organization revealed errors.
- Test results indicated a code was in error.

The types of errors that typically occur are as follows:

- Programming Errors
- Errors in the input (erroneous)
- Errors in the use of the code (wrong applications)
- Models not properly converted to mathematical expressions for code input.

Based on discussions with the vendors inspected in this study, the conclusion is that the majority of the errors reported to date were introduced into the

ECCS codes during the period in which the evaluation models were being developed in accordance with Appendix K to 10 CFR 50. Development of ECCS models at that time was done on a priority basis to meet regulation deadlines, and development and review practices were less than optimum. Moreover, procedures for code development and control that existed at that time were not nearly as detailed as those that exist today. Subsequent to the evaluation models being developed and approved, some vendors did audit their codes again for correctness.

There are numerous errors that are found and corrected by the internal reviews and checking process before the code is submitted to NRC for approval. Unfortunately, none of the vendors has kept any statistics on the number of errors detected during the development versus the numbered detected later. The concensus of the inspected vendors, based on experience and memory, was that the review and checkout procedures for codes caught approximately 95% or more of the errors. Code files examined did reveal internal memos, notes, etc., documenting some error corrections; however, not all error corrections were documented, and those that were did not corroborate the estimated 95%.

5.3 Impact of Errors

Errors found in thermal-hydraulic safety analysis codes can be either conservative* or non-conservative.* These two are addressed for ECCS codes. For transient analysis codes, the error type is not relevant, due to the present lack of reporting requirements (see section 4.3.2).

5.3.1 ECCS Codes

For errors discovered in ECCS codes that are conservative (e.g., a heat generation term inadvertently multiplied 2), the code can still be considered acceptable with a known "conservative" model in it. If the applicant does not wish to take credit for the error correction, then no reanalysis or operating technical specification change is necessary. If credit is to be taken, then reanalyses would be required.

For errors that are non-conservative,* staff practice has been to impose an interim penalty for all operating plants, and to require all of the affected plants to submit recalculations using the corrected model.

Normally, the correction of an error is accompanied by an application for ECCS model change. These changes involve the removal of some conservatisms or conservative features in the ECCS evaluation models that are not required by Appendix K to 10 CFR 50. In the past, these changes usually offset the penalizing effects of the error, with the result being no net change in the operating limits of the plant. As a result ECCS, code errors have historically not impacted the operational limits of affected plants.

---

*"Conservative" means that with the correction, the code predicts less severe results. Non-conservative means that with the correction, the code predicts more severe results.

5.3.2 Transient Codes

To date, only one error has been reported in a transient analysis code. There was no impact on licensing calculations performed with the code because the error only affected the Anticipated Transient without Scram (ATWS) analyses being performed as part of a generic study. Other errors may have been found by the vendors in their transient codes, but they have not been reported to NRC, nor is it required.

Before examining the results of the inspections, a brief discussion of the reporting requirements for errors is given both for ECCS codes and for transient codes.

5.4 Reporting Requirements

5.4.1 Reporting Requirements for ECCS Errors

The requirement for reporting errors in ECCS codes is found in 10 CFR 50.34 (a)(4) and (b)(4):

> "Analysis and evaluation of ECCS cooling performance following postulated loss-of-coolant accidents shall be performed in accordance with the requirements of 50.46 for facilities for which construction permits may be issued after December 28, 1974."

If an error is found in an ECCS code, calculations performed with that code are not considered to be in compliance with Appendix K, and this deficiency must be reported to the Commission.

5.4.2 Reporting Requirements for Computer Codes

With the exception of the reporting requirements for ECCS evaluation model errors noted above, the only requirements for reporting errors found in safety analysis computer codes are those found in 10 CFR 21 and 10 CFR 50.36 regarding operating plants, and those found in 10 CFR 50.55 regarding construction permit applications. The 10 CFR 21 requirements are applicable only if the error resulted in creating a substantial safety hazard, and are quite specific regarding notification requirements once a compliance failure or defect is positively identified. Notification of NRC within 48 hours is required. The part 50.55 requirements are applicable if the error "...were it to remain uncorrected, could have affected adversely the safety of operations of the nuclear power plant at any time throughout the expected life time of the plant..." Notification of NRC within 24 hours is required. However, no time limit is specified regarding how long an organization has to evaluate a potential safety concern in order to establish if the safety concern is justified and should be reported under part 21 or part 50.55.

In the case of the upper head coolant temperature error by Westinghouse,* approximately 4 months elapsed between the time Westinghouse was first informed of a potential code error and the time it was confirmed that there was a code error. Similarly, a period of 9 months elapsed for the evaluation

See Appendix A, Westinghouse Trip Report, enclosure (2) of a Potential Reportable Concern at GE. No documentation was found in either case which justified the amount of time taken to perform the evaluations. However, in the case of the zirconium-water reaction rate error by Westinghouse, only 10 days elapsed between the time Westinghouse was first informed by a company in France using the LOCTA code of a potential code error and the time it was confirmed that a code error did exist. Despite the wide range of evaluation times, the acceptability of the evaluation time is questionable.

In the case of thermal-hydraulic transient codes, reporting is not required as long as reanalyses with the corrected code do not result in previously established technical specification limits being invalidated. (For example, if a minimum departure from nucleate boiling ratio (MDNBR) was originally calculated to be 1.5 and subsequent to correction of an error, it was recalculated to be 1.35, the error would not have to be reported because the recalculated MDNBR was less than the minimum allowable MDNBR value of 1.3).

There also appears to be considerable ambiguity regarding the reporting of not only code errors, but also changes to codes. While a vendor can use a staff-approved code for safety analyses, he can also make a change to that code subsequent to the staff approval and use it without officially notifying the staff. The only way the staff would know a change was made was if the code was not specifically identified as staff-approved in that section of the Safety Analysis Report (SAR) which identifies methods used.

In addition, if an applicant was aware of an error, he would not necessarily be required to report it to the Commission. This is because safety analyses reported in the SAR usually only conclude that results remain above acceptable limits (e.g., "the minimum DNBR does not drop below the 1.25 limit"). Thus knowledge of an error does not invalidate the statement that information in SARs is sworn to be correct to the best of the belief of the applicant as long as limits are not violated. Moreover, there is nothing to stop an applicant from compensating a large error in a transient code by making "improvements" to other areas in the code such that the results obtained with a corrected and "improved" model still do not violate acceptable limits.

Finally, no requirements presently exist for vendors to report any kind of code errors either to the NRC or the applicants unless they are covered by contracture requirements.

Regulatory Guide 1.16, "Reporting of Operating Information--Appendix A, Technical Specifications" clarifies the requirements of 10 CFR 50.36 and identifies types of reportable occurrences that the NRC should be promptly notified of with written followup. This includes "errors discovered in the transient or accident analyses or in the methods used for such analyses as described in the safety analysis report or in the basis for the technical specifications that have or could have permitted reactor operation in a manner less conservative than assumed in the analyses . . ." This guide however, is intended for the operators of a plant, and not the vendors who designed it. Hence, the vendors must report any errors to the applicants or licensees in order for them to be reported in accordance with Regulatory Guide 1.16. As mentioned before, there are no requirements for vendors to report code errors to the applicants.

6.0 Applicable Standards

The quality assurance procedures of all of the vendors are designed to implement the requirements of ANSI (American National Standards Institute) standard N45.2.11-1974, "Quality Assurance Requirements for the Design of Nuclear Power Plants". This standard has been endorsed by the NRC through Regulatory Guide 1.64, "Quality Assurance Requirements for the Design of Nuclear Power Plants." The standard does not specifically state its applicability to computer codes, but considers codes in the same way it would consider a component or system design.

This deficiency has been recognized and efforts are now underway by the ASME Nuclear Quality Assurance Working Group on Design Control to propose an amplification to the design QA practices to provide better guidance specific to computer codes. It is the inlent that this information will be added to ANSI/ASME NQA-1-1979, "Quality Assurance for Program Requirements for Nuclear Power Plants."

In addition, ECCS evaluation model codes must also meet the requirements of Appendix K to 10 CFR 50. These requirements impose uniformity of many aspects of the calculations models and are not QA requirements. However, experience has shown Appendix K to require controls similar to quality assurance procedures.

In addition to ANSI N45.2.11-1974, there are several standards which have been developed or are currently being developed by the ANS-10 Standards Committee of the American Nuclear Society which are described briefly as follows:

(1) "Guidelines for Verification of Computer Programs" provides users with information about the models being represented, the thoroughness of the software testing effort, guidelines for types of information that should be supplied for verification, and information that facilitates modification, maintenance, and transportability of computer codes.

(2) "Guidelines for the Documentation of Computer Programs," ANSI-N413, facilitates the effective usage, transfer conversion, and modification of computer codes.

(3) "Guidelines for Considering User Needs in Program Development," ANSI/ANS-10.5-1979, ensures the proper application and simplifies the use of the code. The intent is to encourage the development of a product that will be easy to apply correctly.

ANSI-N413 and ANSI/ANS-10.5-1979 have been issued and are available to the industry. However, they have not been officially endorsed by NRC through a Regulatory Guide. The need to officially endorse these standards should be explored by NRC.

7.0 Industry Practices

7.1 Code Development and Modification Practices

Many times errors are introduced in a code during its development or modification. This section examines present industry practices in the area of code development and modification.

The primary responsibility for assuring that a code does not contain errors rests with the individual doing the development or modification. The size and complexity of present generation thermal-hydraulic safety analysis codes is such that only the developer truly understands the overall logic that went into designing the code. It usually takes well over a year for a reviewer to learn the code and to gain the same level of insight and understanding as the developer. To do this, the reviewer must work with the code on a full-time basis. Typically, this is not done, due to excessive manpower costs.

Code developers are highly competent individuals because of the complexity of the codes they develop, the impact on safety the results of these coses will have, and the detailed review the codes will be subjected to by NRC. In some organizations, the code developer also programs the equations, models, and correlations into the computer language. In other organizations, there is a separate group of programming specialists who program the code in cooperation with the code developer.

After the basic code is programmed and operational, it undergoes checkout and verification. This is typically performed by the code developer as well. There is no specific set of procedures to follow during this stage of the development and the extent of checkout and verification is usually determined by the developer.

There are various methods for design verification. The three methods discussed in ANSI N.45.211-1974 are design reviews, alternate calculations, and qualification testing.

Some code developers compared their results to similar calculations for previously designed plants, while others used alternative calculations, such as other codes or hand calculations to check their work. In many instances, the modified version of a code was run, the new results compared with the old results, and any changes observed were determined to be consistent with the modification made.

At this point, it is worthwhile to note the verification work that was performed by CE on two of their ECCS evaluation model codes, STRIKIN-II and CEFLASH. The STRIKIN-II code had never been thoroughly reviewed so CE had two relatively new engineers review the STRIKIN-II code. This served both to familiarize the engineers with the code, as well as to find any errors. The review consisted of essentially rederiving the constitutive equations and code logic. As a result of this review, CE uncovered a number of errors, all but one of which had a negligible effect on the calculated peak cladding temperature. Because of the errors found in STRIKIN-II, the same kind of review was done for CEFLASH. No errors were found, and hence nothing was reported.

When asked why they did the review, CE stated that the impact of finding errors in licensing codes was great enough to have them look for errors at that time rather than to have them appear unexpectedly at some later time. They said that if NRC did not place the importance it does on small errors, they probably would not have performed the review. The total manpower expended to review the STRIKIN-II code was about two manyears.

In reviewing the extent of the verification and checkout work in codes, it was difficult to determine what had been done, since generally either the documentation was incomplete or no documentation existed at all. Moreover, the correctness of a code submitted for staff review is not attested to by a signed affadavit at the time of submittal, as is required for all docket submittals.

ANSI N.45.2.11-1974 requires that "design verification shall be performed by any competent individuals or groups other than those who performed the original design but who may be from the same organization." In actual practice, there are essentially two design verifications, one by the code developer and one by an independent verifier. The review by the code developer is much more rigorous than the one by the independent verifier and usually is performed by alternative calculations or methods of verification other than design review.

The independent verification is almost always performed by design review. In some cases, the design review can be quite short. For example, see item B.1 of enclosure (1) to GE trip report of Appendix A.

Many, but not all, thermal-hydraulic safety analysis codes undergo some qualification testing. For ECCS codes, participants in the Standard Problem program compare their codes predictions against experimental systems data such as from the Semiscale, TLTA, and LOFT facilities. (During one inspection, a vendor informally mentioned that they considered the staff audit calculations a form of independent verification.) BWR transient codes are being compared against some tests run at the Peach Bottom BWR plant. These comparisons and results are not considered by most of the vendors to be part of code verification files however. The reason given by the vendors for this with regard to ECCS models is that the ECCS models have been approved by NRC, and therefore are no longer being evaluated by the vendor.

In fact, B&W procedures state that the verifiction requirements are waived when the code is considered consistent with applicable NRC regulations (see item II of enclosure 2 to the B&W trip report in Appendix A). The argument given to justify this waiver is that regulatory requirements usually impose unrealistically conservative assumptions to be made in certain areas so that meaningful comparisons to data would not be possible.

The staff rejects this argument since in most instances the conservative requirements involve specific methods and do not affect the overall structure of the model. Thus, replacement of the individual conservatisms with best-estimate methods would allow meaningful comparisons to test data to be made. Finally, the staff believes that the responsibility to assure the correctness of the plant safety evaluations rests with the licensee.

Qualification testing can only uncover major code errors and not minor code errors. This is particularly true for ECCS codes. Present uncertainty bands on code calculations of cladding temperatures are on the order of a few hundred degrees due to both calculational and measurement uncertainties and three dimensional variations in data. Any errors which impact the results by less than this amount would most likely not be detected based on data comparisons. Therefore, verification by alternate and/or hand calculations would most likely be the best way to determine if small errors exist.

Some vendors have utilized codes that were developed by organizations other than their own. There are no requirements that these codes be developed in accordance with any quality assurance procedures, and it is up to the vendors to assure their accuracy. None of the vendor's procedures distinguish between codes developed within their organization and those developed outside of their organization with regard to verification. Since the major part of code verification is typically done by the code developer, the above methods appear inadequate, and it could not be determined if quality assurance practices in the absence of specific procedures were sufficient for verification of codes developed by others. (See item 2.8 in enclosure (1) of the ENC trip report in Appendix A.)

7.2 Code Use and Control Practices

7.2.1 Code Use

Code users may be either the code developer or others. Errors in code use can be made in a number of ways, such as errors in input data (e.g., the wrong number was inadvertently punched on a card.), input data derivation errors (e.g., the wrong initial upper head fluid temperature) errors in using code results (e.g., a code calculation was prematurely terminated resulting in a wrong output parameter value) and code applicability errors (using a code for a set of conditions for which the code was not intended to be used).

Project ECCS files that document the ECCS calculations for specific plant analyses were examined in a few of the vendor organizations. These files were generally well organized and documented. Input data derivation and traceability to the source was thorough. While verification is performed on the input data derivation information, there does not appear to be any checking or review of this information after it has been transferred to the actual code input (e.g., on punched cards). Most of the ECCS codes however, print out the input data so that the input actually used can be checked as part of the output verification. In some instances, calculations are submitted to NRC before the checkout and verification work is completed and properly documented (see item 2.13 of enclosure (1) to CE trip report in Appendix A).

7.2.2 Code Control

Codes are usually controlled and maintained by a code custodian. The responsibility of the code custodian is to see that the proper, approved, versions are being used for analyses, and that all code modifications are done in accordance with established procedures.

8.0 Observations

Appendix A to this report contains trip reports issued by the Analysis Branch of NRR after each vendor inspection. Appendix B to this report contains inspection reports issued by the Region IV Office of Inspection and Enforcement after each vendor inspection. These reports document specific observations made during the inspections.

8.1 NRR Trip Reports

After each inspection, a trip report documenting the NRR staff's observation was issued and a copy placed in the Public Document Room. Each vendor was advised of the availability of the trip report.

8.2 Region IV Inspection Reports

As stated previously, Region IV inspections have two distinct objectives; (1) to determine if the vendor's procedures fulfill the commitments of the approved quality assurance program, and (2) to determine if the vendors are following their procedures.

Failure to do either of the above is cited by the inspector as a deviation, which requires corrective action including the identification of measures to be taken to prevent recurrence.

At the end of each inspection, the IE inspectors conduct an exit interview with the vendor management, at which the vendor is advised of any deviations found. During the exit interviews for the inspections conducted for this review, the NRR staff also advised the vendors of the staff's observations and any items for their consideration.

Subsequent to each inspection, Region IV issues a formal inspection report to the inspected organization. These reports identify deviations, as well as other items for consideration. The vendors are required to respond within 30 days to any deviations identified. This response must identify the corrective action and any measures to prevent recurrence. Vendor responses to the inspections conducted for this review are provided in Appendix C.

8.3 Deviations

One deviation, the lack of a procedures to report change to the evaluation model to the NRC as required by Appendix K to 10 CFR 50, was found at three of the inspected vendors. This deviation was found during the third of the five inspections, and the two vendors inspected earlier whose procedures were not specifically reviewed for this requirement, were inspected for compliance at the next scheduled inspection (early CY'79)

Other deviations involving failure to follow procedures were found at all of the inspected vendor organizations.

9.0 ACRS Comments

On January 16, 1979, the NRR staff presented its preliminary conclusions and recommendations from the code inspections to the ACRS ECCS subcommittee and its consultants. The Subcommittee commended the NRR staff on its trip reports (Appendix A) and raised numerous questions on the code development process, along with some concerns in specific areas. These were discussed at length, and the subcommittee concerns and comments are considered in the conclusions and recommendations of this report.

There were no unresolved areas of concern. The subcommittee chairman informed the full committee in February, 1979 of the outcome of the subcommittee meeting. The full committee has not requested a briefing by the staff.

10.0 Conclusions

As a result of observing vendor practices in the area of thermal-hydraulic safety analysis code quality control, a number of conclusions were drawn. These conclusions either address the general adequacy of existing controls (section 10.1) or identify deficiencies in present practices and procedures (section 10.2 through 10.4).

10.1 General Adequacy of Existing QA Requirements

A. 10 CFR Part 50, Appendix B and Regulatory Guide 1.64, which endorses ANSI N45.2.11-1974, "Quality Assurance Requirements for the Design of Nuclear Power Plants," are considered acceptable controls for the development and use of computer codes. The licensing procedures and criteria for accepting QA programs are contained in Standard Review Plan sections 17.1 and 17.2, which address the applicability of Regulatory Guide 1.64 (ANSI N45.2.11-1974).

B. Based on review of the vendors' computer code quality assurance procedures, the NRR staff concludes that the vendors' procedures are reasonably uniform in content, scope, and applicability, and are generally acceptable for application to safety analysis computer code development and use. However, there were observed cases where the procedures do not adequately address key elements of the design and safety analysis process. Examples of these, which are discussed in more detail later in this section, are listed below:

   1. Content and organization of code files

   2. Verification

   3. Documentation

C. The vendors are continually revising their procedures to eliminate ambiguities, extend applicability, and, in general to improve them. In some cases it was found that present procedures are the fourth or fifth revisions of procedures that existed four years ago, or that procedures in force today did not even exist four years ago.

D. The staff believes that staff audit calculations of vendor analyses provide a necessary indpendent check on the adequacy of vendor computer models. Previous experience has shown the NRC audit calculations to be beneficial in uncovering errors in vendor models. In addition, they provide increased confidence in the adequacy of vendor models by staff confirmation of vendor analysis conclusions.

E. Among the computer codes audited, the ECCS code files were generally better organized than the non-ECCS code files. This was primarily because of the stricter NRC requirements placed on ECCS codes and the greater attention given to them by NRC.

F. Most of the errors reported to date were introduced into the codes during the code's development, or at times when major revisions were made. In particular, many of the reported errors were made during the initial period of compliance with the ECCS rule (10 CFR 50.46 and Appendix K to 10 CFR 50) in 1974.

G. The codes are generally developed and used in accordance with established procedures and good engineering practices, and it is expected that major errors should have a low probability of occurrence if these procedures and practices are properly followed, and the codes are adequately verified through alternate calculations and qualification testing.

H. The percentage of errors that are found after a computer code is released is small compared to the percentage found during code development and checkout, based on vendor estimates. While no actual statistics exist, the vendors agreed that most of the errors are found during development.

I. Independent verification is primarily by design review. A majority of verification work utilizing methods other than design review is usually done by the developer. Based on the observed vendor engineering practices, independent verification by design review is acceptable if other methods (alternate calculations or qualification testing) are performed as well. The other methods do not necessarily have to be performed independently, however. If independent verification by other methods is feasible however, we would strongly encourage its use.

10.2 Enforcement of Existing Regulations

The following conclusions pertain to area of code development in which ANSI N45.2.11-1974 requires procedures where procedures presently do not exist. Table 10.1 summarizes these areas.

A. Code Identification

In one case, it was found that more than one version of a code existed, yet both versions had the same identification (see item III of enclosure 2 to B&W trip report in Appendix A). The requirement for a procedure requiring appropriate identification of codes and code revisions is identified in sections 4.2 and 4.5 of ANSI N45.2.11-1974.

B. Formal Notification to Code Users of Code Modifications and/or Changes in Code Status

In one case, it was found that the only way code modifications and/or changes in code status were transmitted to the users was by the code custodian informally telling the users, with no formal transmittal

TABLE 10.1

AREAS FOR IMPROVEMENT REQUIRED TO MEET ANSI N45.2.11-1974

	ITEM	REQUIREMENT LOCATION IN ANSI N45.2.11
1.	Procedures for Code Identification	4.2, 4.5
2.	Procedures for formal notification of code users of any code changes and/or changes in code status	8.0
3.	Procedures for Correcting Codes with Errors	9.0
4.	Procedures for follow-up and close-out actions when problems with codes are identified	9.0
5.	Procedure which requires that procedures be examined in the event of an error to determine if the error was caused by a fault of the procedure	9.2
6.	Procedures for documenting verification scope	6.1, 6.3
7.	Procedures for using codes in applications other than those for which the code was originally developed	6.2
8.	Procedures for using codes in overall analysis models (where a model is composed of two or more codes)	6.2

identifying the changes. (See item 3.6 of enclosure 2 to Exxon trip report in Appendix A.) The requirement for a procedure requiring the formal notification to users of code modifications and/or changes in code status is identified in section 9.0 of ANSI N45.2.11-1974.

C. Correcting Codes with Errors and Follow-up Actions When Problems with Codes are Identified

In one case it was found that an organization did not have a procedure requiring the correcting of codes with known errors and another organization did not procedurally control the follow-up and closeout of problems identified with codes (see item B.9 of enclosure 1 of GE trip report and item 2.11 of enclosure 1 of ENC trip report in Appendix A). Both of these items require procedures by section 9 of ANSI N45.2.11-1974.

D. Reexamination of Procedures in the Event of an Error

The staff found that one organization (see item A.9 of enclosure 2 of Westinghouse trip report) did not require that procedures be reexamined to determine if a code error was the fault of the procedures. The requirement for such a procedure reexamination is in section 9 of ANSI N45.2.11-1974.

E. Documentation of Verification Scope

For almost all the vendors, the scope of verification efforts was not documented (see item 3.10, section 2, enclosure 1 of ENC trip report; item B.4, enclosure 1 of GE trip report; item 4.17, enclosure 2 of Westinghouse trip report; and item 2.3, enclosure 1 of CE trip report, all in Appendix A). The requirement for such a procedure, particularly a checklist similar to that found in section 3.2 of ANSI N45.2.11-1974 is in sections 6.1 and 6.3 of ANSI N45.2.11-1974.

F. Use of Codes Outside of Intended Range and in Overall Analysis Methods

Present vendor procedures appear to only address code verification and code use within the context of an individual code being used within its intended range of application. In one instance, it was found that an error resulted because a vendor used a code incorrectly as part of an overall evaluation model (see item C.3 of enclosure 1 of GE trip report). This could have possibly been precluded had a procedure existed requiring the verification effort to consider integral code use as part of a more extensive analysis model (e.g., evaluation model).

Similarly, another vendor applied a transient code to a problem outside of its intended range (see section 4.2.2). It is believed this would not have happened had a code verification procedure been in place requiring verification of code application.

The procedures identified above are considered required by section 6.2 of ANSI N45.2.11-1974.

Since the items identified above are all considered to be required by ANSI N45.2.11-1974, IE will inspect each vendor for these procedures at a future scheduled inspection and require these procedures if they already do not exist.

10.3 Additional Recommendations for Improvement

The following items are presently not required by existing regulations, regulatory guidance, or ANSI standards. As such, they are presented as recommendations for further consideration.

A. Reporting of Computer Code and Analysis Model Errors and/or Deficiencies

10 CFR 21 and 10 CFR 50.55 set forth the requirements for the reporting of defects and noncompliance for operating plants and construction permit applications respectively. In particular, 21.21(b)(2) requires "Initial notification... shall be made within two days following receipt of the information," and that "...if initial notification is by means other than written communication, a written report shall be submitted to the appropriate office within 5 days after the information is obtained."

Part 50.55(e) states, in part, "The holder of a construction permit shall within 24 hours notify the appropriate Nuclear Regulatory Commission Inspection and Enforcement Regional Office of each Reportable Deficiency."

All vendors procedures included a provision for reporting code errors or deficiencies. These were called a PSC (Potential Safety Concern), a PRC (Potential Reportable Concern), or something similar. Potential Safety Concern reports are initiated at the staff level, or above (see item B.10 of enclosure 1 of GE trip report in Appendix A for example).

If the engineer decides that the problem, whatever it may be, is not considered reportable, then it goes no further, with no documented justification as to why it was not reportable.

Of more importance however, is the lack of requirements for vendors to complete the necessary evaluation in a timely manner once a potential concern has been identified. From the vendor design review files examined, these evaluations of potential safety concerns took anywhere from a few days to about 9 months.

The vendors have been found to be in compliance with the requirements of 10 CFR 21 or 10 CFR 50.55, , in that the only time limits they are required to meet are those set forth in 10 CFR 21 and 10 CFR 50.55 from when the potential error or deficiency was judged to be real and reportable.

It is therefore recommended that NRC should consider the establishment of specific time limits for vendor evaluation of potential safety concerns, and requirements for more thorough documentation by vendors of the disposition of potential safety concerns found not reportable. Alternatively, reporting requirements to NRC of potential safety concerns when they are filed in vendor organizations might also be considered. Expansion of any requirements to the industry in general (applicants and licensees) may also be desirable.

B. Errors and/or Model Changes Not Reportable Under 10 CFR 21

Vendors are not required to report any model errors found or changes made to safety analysis codes (see item 2.2 of the enclosure to CE trip report in Appendix A for example). For changes made to previously approved codes, the only way the staff can become aware of the change is if the vendor voluntarily notifies the staff, or if the SAR does not identify the code as staff-approved.

With regard to transient analysis code errors, correction of errors to comply with staff-approved models does not require any reporting of the errors as long as reanalyses with the corrected code do not invalidate any previously approved technical specifications limits. Moreover, the vendors have no requirements to reanalyze with the corrected code all plants whose technical specifications were based on the code with the error.

Even if the vendor does report the error to the applicant, the applicant's sworn affadavit attesting to the correctness of the submitted analyses remains valid because the affadavit attested only that the allowable limits were not exceeded, not that the specific results were correct. Only if the applicant is made aware that the error results in allowable limits being exceeded is he required to notify the Commission that the affadavit is no longer correct. It is recommended that NRC should consider the establishment of specific criteria for the reporting to NRC of errors and modifications in non-ECCS safety analysis codes. In particular, the consideration should be extended to other types of codes (e.g., seismic, structural) as well as Thermal-hydraulic Safety Analysis Codes.

C. Code Classification Levels

All of the vendors have defined code classifications, such as master code, developmental code, conditionally certified code, and fully certified code. While most safety analysis codes have been in use long enough that they should be classified in the highest quality category, in practice most of them remain in classifications less than the highest category (for example, see 3.9 of enclosure 1 of ENC trip report and item VIII of enclosure 2 to B&W trip report, both in Appendix A).

Codes used for safety analyses should be maintained in the highest quality category. It is recommended that NRC consider establishing specific requirements that would require vendor procedures to identify the maximum time a code used for safety analyses can be maintained in less that the highest quality category before it must be recategorized into the highest category.

D. Independent Verification

The majority of code verification was found to be done by the code developer and not by the independent verifier. Most of the independent verification work was done by design review in the case of codes developed internal to the user organization. For codes developed outside of the user organization (e.g., developed by an independent contractor), there is no requirement that the outside organization meet the requirements of ANSI N45.2.11-1974 or that the developer operate under an approved QA program. (See item 2.8 of enclosure 1 of ENC trip report in Appendix A.) The user organization is only required to verify the code, and thus could verify it only by design review. Codes developed external to the user organization should receive verification more extensive than design review only. Therefore, NRC should consider establishment of requirements for independent verification of codes by other means in addition to design review if the code is not developed within the user organization or under an NRC-approved QA program.

E. Code File Index

None of the vendors inspected produced an index of the project or code development files. This made it extremely difficult for both NRR and IE to determine what information was contained in a file (see item 2.1 of the enclosure to the CE trip report in Appendix A for example). Typically, the staff would request information on a code and, as questions arose, the vendors would produce more documents.

If a central index existed listing all documents composing the code design or project file, it would be advantageous to each vendor and also greatly aid NRC during inspections. Therefore, NRC should consider the need for a requirement for vendors to keep central indices for all code design and project files.

F. Code Submittals

In two cases it was found that code analyses results were submitted to NRC for approval prior to completion of all verification work, specifically the signing and dating of forms by the independent verifier. (See item 2.6 of enclosure 1 to ENC trip report and item 2.13 of the enclosure to the CE trip report, both in Appendix A.)

In one case, this practice has been corrected. In the other, confirmation of one or two items was needed to complete verification. However, verification is considered complete only when the independent verifier signs and dates the appropriate form. The staff has always assumed that information submitted for review and approval has been properly verified. Therefore, NRC should assess the need for a requirement that vendors complete all QA requirements through independent verification prior to submitting any information to NRC for review and approval.

As a result of this, the staff intends to confirm early in technical reviews that all verification work has been completed. This will most likely be done through the normal question and answer process.

G. Topical Reports

It appears that while computer codes undergo an independent verification, there is no requirement for the topical reports that describe such codes to undergo a similar independent verification for correctness. Moreover, there are no requirements for vendors to correct errors in the topical reports (see item A.11 in enclosure (2) of Westinghouse trip report). Since the NRC staff presently bases its review and approval of computer codes on the topical reports submitted, NRC should consider the need for requirements for vendors to independently verify the topical reports describing codes submitted to NRC.

H. Extension of Code QA/QC Practices

The inspections performed in this study focused on computer codes from one area of nuclear plant design, namely thermal-hydraulic safety analysis codes. From this, the staff obtained a fair understanding of NSSS vendor and fuel supplier quality assurance procedures for all types of codes. We do not recommend any further investigations in the near future for other types of codes used in NSSS vendor or fuel supplier organizations. However, NRC should consider conducting similar investigations of computer code quality assurance practices and procedures in other areas of the nuclear industry (e.g., architect-engineering firms, utilities, and NRC contractors). In addition, NRC should consider the need to setup internal quality assurance procedures for staff engineering audit calculations.

I. Quality of Information Submitted to NRC

Some of the reactor vendors expressed a view that NRC performed an independent check of their calculations. NRC does not have the capability to independently check all vendor calculations. Staff analyses are of the audit type in selected areas and are not meant to confirm completely the adequacy of a design. Therefore, vendors and applicants (or licensees) should be reminded that they are fully responsible for the quality of their calculations. Moreover, NRC should consider the need for generic submittals, code descriptions, and all engineering calculations to be accompanied by an affadavit from the vendor attesting to the correctness of the information submitted as is required for docket submittals by applicants.

10.4 Additional Actions to be Performed by the Staff

A. NRR-IE Interface

Both the NRR and IE staff benefited from the experience gained in the inspections. In addition, the staff believes that many of the inspected organizations benefited from the NRC's review of their code development procedures.

Based on reviews of vendor code files, the quality of staff review of computer code topical reports could be increased, and the time required to review a code could possibly be decreased if the reviewer had access to a code file during the review (for example, during a scheduled IE inspection). The reason for this is that much information normally not submitted in a topical report exists in the code files. For the most part, the NRR reviewer is not aware of this information and would not ask for it during the normal review. Knowledge of what is in the files would aid the reviewer in developing specific questions (as opposed to a general probing type of question) and would broaden his insight into the code development. In addition, the NRR reviewer could assist the IE inspectors to determine specific areas they should inspect.

Based on the above, the NRR staff intends to work with IE more closely during inspections of vendor code development practices.

B. IE Procedure Development

IE utilizes inspection procedures in conducting inspections. No procedures provide specific guidance, however, on the inspection of computer code development and use, particularly in identifying what areas should be inspected and to what depth. Since an inspector is not expected to be aware of detailed problems or areas of concerns NRR may have with codes, an inspector's conclusion that a procedural requirement has been met does not necessarily mean that the work is either applicable or complete. For example, all that may be required procedurally to demonstrate that a code has been verified is a signature of the independent verifier. The IE inspector would find this acceptable since this is all the documentation required by the procedure. However, the verification work done may be wholly inadequate or insufficient for the problem at hand. With an inspection procedure specific to computer codes, then more detailed guidance would be available to the inspector regarding what areas should be inspected in more detail than others, what areas are of more concern than others, etc.

Therefore, the IE staff will consider developing inspection procedures for computer code development and use.

C. Review of Additional ANSI Standards

In addition to ANSI N.45.2.11-1974 endorsed by NRC, there are two additional ANSI standards presently available which pertain to quality assurance for computer code development and use. These standards have not been endorsed by NRC however.

Therefore, NRC should review ANSI-N413, "Guidelines for the Documentation of Computer Programs" and ANSI/ANS-10.5-1979, "Guidelines for Considering User Needs in Program Development." If found useful and acceptable, these standards should be officially endorsed by NRC through issuance of a Regulatory Guide.

D. Requirement Clarification

As stated previously, the applicability of ANSI N.45.2.11-1974 to computer code development and use has not been clearly defined. IE initially did not consider certain recommendations for procedures as required by existing regulatory guidance. Subsequent interpretation by the Quality Assurance Branch, NRR has determined these recommended procedures are required by ANSI N45.2.11-1974. The Quality Assurance Branch has taken steps to provide clearer guidance in the Standard Review Plan as to the controls that apply to the development and use of computer codes. Specifically, the controls being required in Chapter 17 (Quality Assurance Program) of Safety Analysis Report by the revised Standard Review Plan are as follows (the underlined sections indicate revisions);

1. Activities related to Quality Assurance Program (17.1.2) are acceptable if:

   c. A commitment that the development, control, and use of computer code programs will be conducted in accordance with the QA program and a description of how the QA program will be applied.

2. Activities related to Design Control (17.1.3) are acceptable if:

   3A The scope of the design control program includes design activities associated with the preparation and review of design documents including the correct translation of applicable regulatory requirements and design bases into design, procurement and procedural documents. Included in the scope are such activities as field design engineering; physics, seismic, stress, thermal, hydraulic, radiation, and the SAR accident analyses; associated computer programs; compatibility of materials; accessibility for inservice inspection, maintenance, and repair; and quality standards.

   3B Organizational responsibilities are described for preparing, reviewing, approving, and verifying design documents such as system descriptions, design input and criteria, design drawings, design analyses, computer programs, specifications, and procedures.

   3C1 Errors and deficiencies in approved design documents, including design methods (such as computer codes) that could adversely affect structures, systems, and components important to safety are documented; and action is taken to assure that all errors and deficiencies are corrected.

   3E2 Procedures are established and described for design verification activities which assure the following:

      c. Procedural control is established for design documents that reflect the commitments of the SAR; this control differentiates between documents that receive formal design verification by interdisciplinary or multi-organizational teams and those which can be reviewed by a single individual (a signature and date is acceptable documentation for personnel certification). Design documents subject to procedural control include, but are not limited to specifications, calculations, computer programs, system descriptions, SAR when used as a design documents, and drawings including flow diagrams, piping and instrument diagrams, control logic diagrams, electrical single line diagrams, structural systems for major facilities, site arrangements, and equipment locations. Specialized reviews should be used when uniqueness or special design considerations warrant.

3E4 Procedures are established to assure that verified computer codes are certified for use and that their use is specified.

Activities related to Document Control (17.1.6) are acceptable if:

6A1 The scope of the document control program is described, and the types of controlled documents are identified. As a minimum, controlled documents include:

a. Design documents (e.g., calculations, drawings, specifications, analyses) including documents related to computer codes.

Activities related to Nonconforming Materials, Parts, or Components (17.1.15) are acceptable if:

15.1 Procedures are established and described for identification, documentation, segregation, review, disposition, and notification to affected organizations of nonconforming materials, parts, components and as applicable to services (including computer codes) if disposition is other than to scrap. The procedures provide for an independent review of nonconformances, including disposition and closeout.

APPENDIX A

NRR TRIP REPORTS ON VENDOR
INSPECTIONS

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

NOV 17 1978

MEMORANDUM FOR: Z. R. Rosztoczy, Chief, Analysis Branch, DSS

FROM: B. W. Sheron, Analysis Branch

THRU: L. E. Phillips, Section Leader, Analysis Branch, DSS LEP

SUBJECT: TRIP REPORT: INSPECTION OF ENC QA CONTROLS FOR SAFETY ANALYSIS CODE DEVELOPMENT

Enclosure (1) documents the report of the trip which Paul Norian, Rene Audette, and I took to ENC on October 31 - November 2, 1978. The purpose of this trip was to accompany the Region IV inspector (D. Anderson) on their inspection of ENC's QA controls for Safety Analysis Code Development in the thermal-hydraulic area.

The observations reported in Enclosure (1) are consistant with the inspection report. While these observations may imply recommended changes to the procedures, it is not the intent of this report to put forth such recommendations. The final report documenting the results of the entire review will present any recommendations and conclusions.

Brian W Sheron
Brian W. Sheron
Analysis Branch
Division of Systems Safety

Enclosure:
As stated

cc: R. Mattson
R. Tedesco
T. Novak
K. Kniel
R. Brickley, Region IV
D. Anderson, Region IV
C. Hale, Region IV
W. Rutherford, IE
A. Bates, ACRS
W. Lyon, RES
W. Haas, DPM
J. Gilray, DPM
S. Hanauer, EDO
P. Norian
R. Audette
PDR

Contact
NRR:B. Sheron
Ext. 27588

ENCLOSURE 1

1.0 Introduction

On October 31 - November 2, 1978, P. Norian, B. Sheron, and R. Audette accompanied D. Anderson of Region IV on an inspection of ENC's QA controls for Safety Analysis code development in the thermal-hydraulic area.

The two computer codes originally intended to be inspected were RELAX and PTS-BWR. It was learned that the RELAX code was still under development and that very little documentation was available. RELAX's predecessor, RELAP, was therefore looked at.

The PTS-BWR code is used to predict the transient behavior of BWRs for non-LOCA events. RELAP is used to calculate the blowdown and the reflood hydraulics of the LOCA accident. Unlike previous inspections, Exxon has not reported any code errors to date, and therefore no examples of previous errors were traced through the procedures.

2.0 Areas for Consideration by Exxon Management

The following 15 items were identified to the Exxon management for consideration at the end of the inspection, and are documented as follows:

1. There are no formal procedures for the documentation, timely assessment, and resolution of potential safety concerns, nor are there any procedures for reporting ECCS model changes per the requirements of 10 CFR 50, Appendix K.
2. There are no procedures considered by Exxon to be applicable to code development. Existing procedures are only considered applicable to code use.
3. Verification information should be documented in the project files. Exxon also stated that Management signatures on topical report constituted verification by design review. We do not believe this to be an acceptable

method of verification.

4. When changes are made to the code, letters to code users informing them of the change(s) should be issued and included in the code file. When code versions are approved, the approval letters should be kept in code file.
5. In some instances, signatures indicating that independent checks were performed on final calculations were not found.
6. It was found in some cases that input data calculations were dated after the ECCS analyses were completed and the topical report approved by Exxon Management and submitted to NRC. Independent checks were dated as much as three months after Management approval. (This was found by Exxon in previous internal audits and corrective action taken.)
7. There is no procedure which requires input data, as it is put into the code, to be independently checked.
8. Exxon should have procedures specific to how codes developed by Exxon contractors are to be checked out and verified by Exxon. These procedures should be more specific than those that presently exist in the area of verification requirements.
9. Procedures do not exist which describe the detailed preparation, development, review, approval and control of computer codes.
10. Procedures related to code development activities should address the details of preparation, completion, checking, signing, identification, indexing, etc. of calculation forms.

11. Procedures do not address how Master codes which contain admitted errors, are to be flagged and corrected.

12. The categorization of codes into three classes; master, developmental, and special, does not appear to be sufficient to assure protection of NRC-approved codes. More specific categorization which provides better protection of NRC-approved codes against unauthorized modification is recommended.

13. There is no evidence that code design and project files are indexed, nor is there any requirement that they be indexed. Without indexing, there is no record of what documents constitute a code design or project file.

14. Definitions in procedure XN-NF-S00,002 should be more extensive, encompassing such items as verification, qualification, etc...

15. In some instances, calculational files are only signed by the checker on the first page. This signature is intended to indicate that all pages of the calculation were checked. Better confidence that all pages were checked would be obtained if (1) all pages were signed, and (2) the checker documented in a brief statement the extent and scope of the check.

3.0 <u>Other Observations</u>

3.1 Exxon does not consider their procedures applicable to computer code development, but only to use. The code custodian normally makes a change to the code and checks out the effect of the change himself. The independent verification comes about with code use. At the time the code is used, the independent checker verifies all changes made previously. It does not appear that the reviewer could even determine what, if any, previous code changes had on the answer.

3.2 Code changes made are documented in a notebook entitled "RELAP Documentation UCC". They contain a code listing showing the updates, and a comparison of the results to a standard case in order to determine the effects. The standard case is supposedly a short running problem which tests many of the RELAP features. The comparisons are made at 0, .2, .5 seconds of transient time. The theory is that minor effects on the standard case will be minor for a big plant. Conversely, large effects on the standard case are further investigated with large plant analyses.

3.3 For the ECCS analyses of the R. E. Ginna plant, the input data derivation from SAR information was well-documented and signed by both the developer and checker. Any comparison of the results however, with other data, (i.e., previous calculations, etc.), was not documented. There was no signed calculational form that the output was reasonable, or that it was independently verified. Exxon stated that the Manager signoff signatures on the first page of XN-NF-77-58 (ECCS Analysis for the R. E. Ginna Reactor with ENG WREM-II PWK Evaluation Model) constituted the signature of the verifier(s).

?.4 The design file contained all changes (version) to the code. For changes which were made but not submitted to NRC, documentation was not thorough. However, when a future version was submitted to NRC, all previous changes were included, and the design file contains applicable pages of the submittal in which all changes were described.

Approval letters from NRC are not included in the files however.

3.5 For the GINNA analyses, the TOODEE calculations have the place on the computer output for the preparer and checker to sign. No signatures were found per 6.8.1 of XN-NF-500,002. Also, no places for signatures were found on the RELAP calculations, and no calculational forms (signed) were found, per XN-NF-SOO,002.

3.6 The design record file did not contain internal letters informing user's of code modifications as they are made. The code custodian should issue such a letter.

3.7 When Exxon takes over responsibility of code, then it falls under QA. Exxon does have design reviewers with the contractors, but they are not required by procedures.

3.8 Exxon stated that when code changes are contemplated, a staff meeting is held to discuss the proposed changes. Changes are put into the code by either the engineer who proposed the change, or the code custodian. There is no formal documentation of the change except what the code custodian puts into his notebook, and no letter is issued to code user's informing them of the change.

3.9 Exxon stated that RELAP will always be a developmental code because it cannot meet Master code standards. There is no requirement for controlling developmental codes or for defining how long a code can remain in the developmental stage.

3.10 Exxon management also checks work before it goes out which is a third review and above the normal development review and independent verification.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

B. Sheron

OCT 0 3 1978

MEMORANDUM FOR: Z. R. Rosztoczy, Chief, Analysis Branch, DSS

FROM: B. W. Sheron, Analysis Branch, Reactor Analysis Section, DSS

THRU: L. E. Phillips, Section Leader, Reactor Analysis Section, Analysis Branch, DSS LEP

SUBJECT: TRIP REPORT: INSPECTION OF B&W QA CONTROLS FOR SAFETY ANALYSIS CODE DEVELOPMENT

Enclosures (1) and (2) comprise the report of the trip which you and I took to B&W on 8/29-9/1. The purpose of this trip was to accompany the Region IV inspector (R. Brickley) on his inspection of B&W's QA controls for Safety Analysis Code Development in the thermal-hydraulic area.

Enclosure (1) summarizes the overall observations of their code QA control, and Enclosure (2) provides more detailed information on specific observations. These observations are consistent with the inspection report. While these observations may imply recommended changes to the procedures, it is not the intent of this report to put forth such recommendations. The final report documenting the results of the entire review will present any recommendations and conclusions.

Brian Sheron

Brian W. Sheron
Analysis Branch
Reactor Analysis Section
Division of Systems Safety

cc: R. Mattson	A. Bates, ACRS
D. Ross	W. Lyon, RES
T. Novak	W. Haass, OPM
K. Kniel	J. Gilray, OPM
R. Brickley, Region IV	S. Hanauer, EDO
D. Anderson, Region IV	PDR
C. Hale, Region IV	
W. Rutherford, IE	

Contact: B. W. Sheron, NRR, X27588

Enclosure 1

Summary of Overall Observations

The inspection plan was to audit one ECCS code and one transient code. The codes selected were the THETA code (ECCS hot pin) and TRAP code (steam line break). In addition, a review of circumstances which led to the discovery and correction of 3 previous code errors was also performed. The audit started with the TRAP code, and it was soon realized that [redacted] in order to do a thorough audit, additional time would be needed for the TRAP code, and it was decided to eliminate the THETA code audit from the inspection. Early development of the TRAP code (about 1972) was not based on the procedures that exist today, but on what appeared to be less definitive procedures that existed at the time the code was initially being developed.

Comparisons between procedures which existed then and now pointed out the developmental nature of the procedures, in general. While some weaknesses existed in early documentation requirements, there was evidence that sound engineering practices were probably followed despite a lack of documentation.

The basic concerns in the procedures appeared to be in the areas of independent review and verification, the details of which are discussed in Enclosure (2).

It is also noted that the documentation files showed that during the development of the code, numerous errors were discovered and corrected and/or modifications and improvements made as part of the development process.

Of the three errors looked at there was no basic pattern observed or conclusion reach on either the nature of the errors, or the method of discovery. Stricter procedures might have caught these errors, but it cannot be said with any certainty. At the conclusion of the meeting, Z. Rosztoczy informed B&W management of the NRR observations (no obligation on B&W's part to revise their procedures based on these observations), and R. Brickley presented the inspection findings.

Enclosure 2

Results of B&W Inspection 8/29-31/78

A. General Observations

I. Role of Independent Review in the Development and Modification of Computer Codes

Numerous errors have been found in the TRAP code during last year. Most errors found "coincidentally" and after the program has been released by Technical Staff for production use.

Present B&W procedures do not require independent review of equations, models and/or methods prior or subsequent to programming. Present practice is to appoint same person (cognizant engineer) for both jobs; development of methods, equations, etc., and reviewing the program for use. Selection of independent reviewer for second job has potential to reduce number of code errors going undetected.

II. B&W procedures require a computer code be verified by, in part, a comparison of at least 2 independent cases using the program and comparison with at least one of the following:

a) Experimental Results

b) Closed form solution

c) Results of other accepted codes.

When program is considered consistent with applicable NRC regulations and regulatory guidelines, a, b, c above are waived. This appears inconsistent with the requirements of ANSI standard N45.2.11 as well as with Appendix K to 10CFR50. The responsibility to assure the correctness of the plant safety evaluation rests with the applicant; independent of how detailed Regulatory requirements are, even in cases where Regulatory requirrments are purposely unrealistic in some respect. The computer code can still be checked against experimental data, for example, by bypassing certain models in the code. Verification of these codes (under requirements of Appendix K) is considered equally important as verification of other safety analysis codes.

III. Termination of Certification

No procedure exists which specifies how to terminate a code version which has been found to be in error or has been superceded by a new version. Numerous versions of the TRAP code were certified for use concurrently with others which have known errors.

Formal, well documented procedures should exist for the termination of certification.

Corrected versions of the code should be clearly identified by different version number or equivalent.

IV. Certification Documentation

Present procedures do not require a central certification file for computer codes. Individual code files are kept at different locations.

The present procedure (NPG 0902-06) requires the selection of a representative test case and the placement of this test case in the certification file. As modifications are made to the program, the calculations used to verify the modification have to be placed in the certification file. In the case of full or conditional certification, it is also required that the applicable staff manager or engineer, respectively place original documentation in the certification file. Original documentation, however, is not defined in the procedures.

The above requirements are not sufficient to establish the documentation requirements for certified computer programs. More detailed information, as described below, and/or a more detailed listing of documents which should be placed in the certification file should be defined.

Form PDS-21177, Computer Program Certification, does not require any documentation of what is being certified, including what change was made to the code, why it was made, etc... The certification form should include this information. Form PDS-21177 also requires only the technical staff manager sign the conditional certification, whereas for full certification, the signature of the cognizant programer, cognizant technical staff engineer, and the technical staff manager are required. The signatures required for full certification should be required for conditional certification.

V. Procedures do not address reporting of model changes or errors in accordance with Appendix K, nor do they address reporting of non-ECCS code errors. Moreover, Procedure NPG-0902-06 does not require documentation of analyses performed to justify dismissal of a safety concern.

VI. The procedures only require fully certified codes contain a representative test case to be placed on microfiche in the certification file, with no similiar requirement for conditionally certified codes.

VII. The code manual used in the design section by the design staff does not agree with the manual in the code certification file and neither are up to data. No procedure exists for the code manual to be a controlled document.

VIII. The purpose of conditional certification is to permit use of a code while code verification is being completed. Accordingly, conditional certification is given for specified time period. B&W appears to routinely extend conditional certification expiration dates without having a verification program under way. This is considered inconsistent with the purpose of conditional certification.

IX. When errors were found which affect more than one certified version of the code, corrections in various versions were not clearly documented. The possibility exists for some uncorrected versions to still be available for use.

X. The present procedures are not clear whether calculations performed to verify changes and corrections are required to follow existing procedures (NPG-0402-01) for processing of NPGD Prepared Calcu tions.

B. Observations from TMI-2 and Bellefonte inspections:

a) Individual calculations when they are performed are not certified correct and are not signed by independent reviewer.

b) When a final calculation is completed (could take more than a year), the originator signs form BWNP-20210, a reviewer is also assigned for an independent review and signs the same form.

c) In both the TMI & Bellefonte cases the results of the (SAR) calculations were released by B&W to the utility prior to the originator and the reviewer signing the appropriate form.

d) Design calculations must follow NPG 0402-01. Calculations performed for the safety analysis of the plant and in support of licensing of the plant which are not design calculations, in B&W's opinion do not fall under any of the present procedures.

e) If PSC (Potential Safety Concern) is not filed, there is no procedure for (1) determining the impact of the error, and (2) the correction of the error.

C. Inspection of Example Deficiences Previously Discovered

I. Small Break LOCA Analysis

The worst break location in small break analyses discovered in April, 1978 was the result of an incomplete examination of the small break spectrum when the calculations were performed in 1972-73. B&W, at the time, did not recognize the relationship between break area and break location.

The worst case break location was discovered during the course of generic calculations on small breaks by two individuals. As a result, a PSC was filed due to the indicated significance of the error but prior to the evaluation being completed and QA'd. The NRC was also notified prior to formal management approval of the evaluation. In general, the notification of NRC was prompt, within a few days of where the new break was first discovered.

B&W did not feel that the present procedures would have uncovered this error, although better record-keeping might have helped. In addition, B&W stated they examined their present procedures for areas of possible improvement and stated none were found. Present practice was stated as a technical review by the manager of these types of calculations, which would include reviewing the bases upon which the break spectrum was selected. The actual review process was unclear for this type of situation, since it is a user-oriented type of problem which the procedures do not address.

II. Gravity Head Sign Error

The gravity head sign error was discovered in the process of changing over from version 5PP to version 7 of the CRAFT2 code. Calculations resulted in the peak cladding temperature changing by greater than 20°F, from which it was decided to notify NRC.

B&W did not know how the error got into the code. The code was generally checked in 1974, but the error was not discovered.

B&W's procedures do not require line-by-line checking of codes, but it was felt that line-by-line probably would have caught this error.

Present practice sometimes includes a line-by-line check of code modification, but no existing procedure requires this, and no documentation is required.

For this error, a PSC was not filled out. B&W (Dunn) does not believe that non-compliance with Appendix K is necessarily a safety concern.

The licensing section was informed however, since it was considered a generic issue. A period of about five months elapsed between the time the error was discovered to have a greater than 20°F impact and the time the NRC was informed. Individual plants were not notified, since, in B&W's opinion the corrected calculations indicated no plants would exceed 2200°F. Since no PSC was generated, no file on this error was kept. Documentation of the B&W findings is not available.

The present procedures do not require reporting those errors which were not identified as a PSC to the customers.

B&W did not reevaluate or revise their procedures to insure a better review of programs, and did not give a thorough review to the CRAFT2 code based on finding these errors.

III. Three-Mile Island Steam Line Break Analysis

Previous (1976) Chapter 15 (Appendix 15B) steam line break calculations were based on the FLASH-P code. RADAR code calculations did not show any DNB occurring in the core. Later analyses using the TRAP2 and RADAR codes predicted 15% of the core went into DNB. Based on experience, B&W attributed this difference primarily to differences between the TRAP2 and FLASH-P codes. The FLASH-P code was originally used since it had an interim certification and TRAP2 was not certified. The TRAP2 code is B&W's code for steam/feed line break analyses and has been submitted for review in August, 1976. The FLASH-P code was never submitted for review.

After the differences were noticed, B&W re-reviewed the models in TRAP and concluded they were conservative, but were unable to quantify the conservatism. No PSC was filled out because B&W did not believe the cladding integrity had been violated even though 15% of the core experienced DNB.

NRC rejected this argument and required that all pins with DNBRs less than 1.3 be assumed failed.

B&W did not inform its customers of this difference and based on the TMI results, other plants were not recalculated with the TRAP2 code.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

DEC 0 2 1977

MEMORANDUM FOR: Z. R. Rosztoczy, Chief, Analysis Branch, DSS

FROM: B. W. Sheron, Analysis Branch, DSS

THRU: L. E. Phillips, Section Leader, Analysis Branch, DSS LEP

SUBJECT: TRIP REPORT: INSPECTION OF GE QA CONTROLS FOR SAFETY ANALYSIS CODE DEVELOPMENT

Enclosure (1) documents the report of the trip which you, Jack Guttman, and I took to GE on 9/11-9/14. The purpose of this trip was to accompany the Region IV inspectors (R. Brickley, D. Anderson) on their inspection of GE's QA controls for Safety Analysis Code Development in the thermal-hydraulic area.

The observations reported in enclosure (1) are consistent with the inspection report. While these observations may imply recommended changes to the procedures, it is not the intent of this report to put forth such recommendations. The final report documenting the results of the entire review will present any recommendations and conclusions.

Brian W. Sheron

Brian Sheron
Reactor Analysis Section
Analysis Branch
Division of Systems Safety

Enclosure:
As stated

cc: R. Mattson
R. Tedesco
T. Novak
K. Kniel
R. Brickley, Region IV
D. Anderson, Region IV
C. Hale, Region IV
W. Rutherford, IE
A. Bates, ACRS
W. Lyon, RES
W. Haass, DPM
J. Gilray, DPM
S. Hanauer, EDO
PDR
J. Guttman
J. Spraul

Contact
NRR:B. W. Sheron, Ext. 27588

ENCLOSURE (1)

A. Introduction: Overall Observations

The inspection plan was to audit two ECCS codes and two transient codes. These were the CHASTE, REFLOOD, ODYN, and REDY codes. The CHASTE code calculates the hot pin heatup, REFLOOD the reflood dynamics, and both REDY and ODYN calculate the steam line break accident and other transients.

Similar to previous experience, it was found that only two codes (the ECCS codes) could be properly inspected in the time available. It was found that early development of these codes was based on procedures not in effect today. The basic concerns in the procedures appeared to be in the areas of independent review and verification.

In addition to the above codes, the staff also examined four code deficiencies previously reported to NRC. These were 1) reflood vapor venting logic, 2) the core pressure drop for leakage flow, 3) the minimum pressure used for reflood calculations, and 4) the Peach Bottom tests. The purpose of this was to determine the cause of the deficiency, (i.e., not following a procedure) and to see if any improvements in the procedures would help prevent its recurrence.

B. General Observations

The observations that follow were based on the staff's review of the existing procedures, and are only for consideration by GE at this time.

1. Present procedures are not clear on independent verification requirements. There is no requirement to check the formulation

of equations to be programmed. The programming is checked but is acceptable if the programmer himself performs the checking. The programmer himself can also be the responsible engineer generating the equations. Thus the entire code change can be initiated, accomplished and checked by one single person. This was the case for the various versions of the REFLOOD code. A later step in the process requires review and verification by a committee (Methods Review Committee or Design Review Committee). The Methods Review Committee typically spends less than 30 minutes on a code review and recommendation. The committee, to a large extent, bases its opinion on the information presented to them (verbally) by the cognizant engineer. The computer findings are reported in brief statements without identifying the material reviewed, the extent of the review, or the reasons for the findings. Neither do they specify the restrictions placed on the use of the code. When a design review committee is appointed, a design review report is prepared.

2. It did not appear that the design review team required that they review the resolution of all open items found during their verification review, based on the CHASTE 06 report.

3. Section 4.1 of EOP 40.6.00 requires the code developer to send the design package to the verifier for review. The procedure does not state whether this requirement must be formally documented, and no records in the CHASTE-06 file indicate that this was done prior to the CHASTE-06 design review team verification meeting.

4. Procedure EOP 40.600 spells out requirements and responsibilities for the code developer, verifier, and responsible manager. For the developer, this includes identification of the verification method. For the responsible manager, this includes (1) concurrence with verification method (2) designation of verifiers and (3) review of total verification. The procedures do not require all actions on the above items to be documented.

   Thus there is no traceability as to what verification method was used, and whether the management concurred in the meth^d.

5. GE's procedures (EOP 40.300) specify that a level 2 production code must be verified, but not necessarily qualified. Since GE defines qualification as the measure of how well the calculation compares to data, it appears they have no formal requirement to compare their codes to applicable data. Item A1-3 of Appendix A to EOP 40.6.00 discusses the use of test data in the verification process, but there is no requirement to use this method.

6. EOP 40.6.00 (Independent Design Verification) issued 7-77 requires that the v rifier perform certain steps as part of the verification process. This includes the preparation of a verification statement attesting to the verification, including (1) the identification of the document verified, (2) the name and signature of the verifier and the verification data, (3) a description of the extent and depth of the verification, and (4) a statement of the results of the verification. Not all of the information as required by EOP 40.6.00 section 4.2, was found in the documentation file for the CHASTE-06 code.

7. There is no requirement to retire a code that is known to have errors. Codes (including level 2 codes) are used with errors. Furthermore, GE will not retire a code unless NRC has approved the new version of the code. Warning is not provided to users of the erroneous code.

8. There is no formal distribution of code certification changes. Users learn of certification changes by talking to the cognizant engineer.

9. There appeared to be, in general, insufficient documentation. Concerns, opinions, recommendations were expressed by various people involved in the review process. In most of these cases, a followup does not exist in the file. There are many open items unanswered. The actual changes from one version to the next are not described or referenced in the file.

10. There appears to be a lack of procedures to handle corrections of errors which are not identified as a Potential Reportable Concern (PRC). Errors found in certified codes are not reported in a traceable manner. There is no notification to users. There is no documentation of the correction. One of the sample cases reviewed was identified as PRC's, and documentation was very brief, if any.

11. PRC procedures do not seem to guarantee a timely resolution and reporting of the identified problems. Procedures permit evaluation of the problem for years without a finding and without reporting.

12. In reviewing to find out how did the "errors" slip through the normal QA procedures, two out of the four looked at did not go through a verification process (no design review). One was properly identified as early as 1975, but followup work indicated to GE that there was no problem. More recent tests verified the original findings. The fourth item falls in a category, where there were no formal procedures at the time, but established practice included a check by supervision.

13. Design record files are not defined. At the beginning of a review the subject organization provides the file; later on, as questions are raised, other documents are produced from various sources and are in some occasions inserted in the file.

14. The CHASTE-06 design review on the gamma smearing model was held 9/23/77. Closure of a design review team open item stated CHASTE-06 application would be restricted until the review was closed. No document was found identifying what restriction would be placed on the code in this interim.

C. <u>Code Deficiencies</u>

1. <u>Reflood Vapor Venting</u>

   The venting logic was put in the code when the code was developed. The error was found in October, 1976 by the user doing analyses on plants, in which he noted an inconsistancy in the results. A more detailed review located the error, which probably occurred because the code was not given a detailed design review when it was developed. GE believes that today's procedures would have caught this error.

They did not reassess their existing procedures for adequacy subsequent to discovery of this error. Moreover, they did not reverify the code to determine if additional logic errors exist.

The method by which the error was discussed was that the user discovered the anomaly, and went to the code developer to find out why. A joint comparison study was performed which identified the error. The code developer stated he wrote a letter on the error, but replaced it with the letter which notified NRC of the error. The question was raised as to whether the affadavit signed by utilities on correctness of analysis is correct, since GE may know of a small error. It appears that GE does not feel they have to report small errors to customers (i.e., <20°F) unless a large (>20°F) error is found. There is no requirement in EOP's for engineers to report any errors discovered.

2. Core Pressure Drop for Leakage Flow

GE assumed that the driving head for the liquid entering the lower plenum from bypass channels was due to gravity effects only, and that the pressures in the upper and lower plenums were the same. This assumption was based on steam flow pressure drops through a fuel bundle. What was not considered was that under conditions of counter-current two-phase flow, the pressure drop is not negligible and could be as high as 1.0 psi. Data, supporting the higher pressure drop under counter-current two-phase flow conditions was available, but not to the code developers as it was obtained in other parts of the organization.

3. Pressure Rule

GE stated this error occurred because the behavior of the results was assumed before results were available. GE assumed a constant system pressure during the REFLOOD calculation, and it was obtained from a SAFE code calculation at bottom of core recovery (BOCREC). It was discovered that under certain conditions, lower pressures would be predicted after BOCREC. Since the minimum pressure is most conservative, GE was not always using the most conservative pressure in their calculations. It was pointed out that review process only reviews individual codes, but does not review models, which can be made up of a number of codes. This was an area where the design review group might have looked but probably didn't, and no specific code integration review was made, nor was it required by the procedures. In addition, no design procedures existed at the time the problem was discovered. The present procedures still do not require the review and certification of analytical methods as compared to computer codes.

4. READY Errors Indicated by Peach Bottom Tests

READY is a BWR thermal hydraulic transient code used for the evaluation of anticipated transients like turbine trip. When the READY code was developed years ago, present procedures were not in effect at that time. Nevertheless, equivalent procedures were used.

GE experienced difficulties with the code in 1974 and early 1975. It became obvious that the steam line representation in the code was oversimplified and inappropriate. The responsible GE manager reported the steam line deficiency as a Potential Reportable Concern (PRC). The steam line representation was corrected during the summer of 1975, but the corrected version of the code gave less favorable results. Following the correction a design review committee reviewed the code. The committee concluded that the code was not appropriate for licensing applications even in its corrected form. Additional experimental verification was needed before the code could be used.

GE did not inform NRC or GE's customers of their finding and continued using the uncorrected version of the code in licensing applications. In 1976, based on comparisons with calculations performed by a Scandinavian code (RAMONA), GE decided on continued use of the code again.

In the meantime, GE initiated the development of a new, improved code (ODYN) and initiated tests. The tests were conducted in April 1977 on the Peach Bottom plant in cooperation with EPRI and Philadelphia Electric. The test results indicated significant errors in the READY code. GE continued use of the code and intends to do so until the NRC review of ODYN is complete.

D. Code Use

1. GE keeps a master file for each plant in which all ECCS calculations are documented. A single form is used to document the run number and other key identification information. The documentation of input, including who performed the deck setup, as well as who verified it, is provided through initials of the individual on the form. The documentation of the results review and verification are provided for in the same manner (individual initials and dates form).

The form also provides for documentation of observed differences from any previous calculations.

If errors are discovered in the code inputs, and are not corrected prior to the calculation being released, the user is to notify his management of the error, but is not required to do this formally. Any PRC issued is done so by the manager and not by the staff engineer. PRC's can be initiated by a staff engineer, but are formally issued by the section manager, which is a 3rd line management position above the subsection and unit managers. If a manager does not agree with the staff engineer's concern and doesn't concur in the PRC, then the staff engineer can appeal such a decision up to the company vice president, or he can write NRC directly.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

OCT 12 1978

MEMORANDUM FOR: Z. R. Rosztoczy, Chief, Analysis Branch, DSS

FROM: B. W. Sheron, Analysis Branch, Reactor Analysis Section, DSS

THRU: L. E. Phillips, Section Leader, Reactor Analysis Section. Analysis Branch, DSS LEP

SUBJECT: TRIP REPORT: INSPECTION OF WESTINGHOUSE QA CONTROLS FOR SAFETY ANALYSIS CODE DEVELOPMENT

Enclosures (1) and (2) comprise the report of the trip which Norm Lauben, Wayne Hodges, and I took to Westinghouse on 09/11-09/14. The purpose of this trip was to accompany the Region IV inspectors (R. Brickley, D. Anderson) on their inspection of Westinghouse's QA controls for Safety Analysis Code Development in the thermal-hydraulic area.

Enclosure (1) summarizes the overall observations of the inspection and enclosure (2) provides more detailed information on specific observations. These observations are consistent with the inspection report. While these observations may imply recommended changes to the procedures, it is not the intent of this report to put forth such recommendations. The final report documenting the results of the entire review will present any recommendations and conclusions.

Brian W. Sheron

Brian W. Sheron
Reactor Analysis Section
Analysis Branch
Division of Systems Safety

cc: R. Mattson	W. Lyon, RES
F. Schroeder	W. Haass, DPM
T. Novak	J. Gilray, DPM
R. Brickley, Region IV	S. Hanauer, EDO
D. Anderson, Region IV	PDR.
C. Hale, Region IV	W. Hodges
W. Rutherford, IE	N. Lauben
A. Bates, ACRS	B. Sheron

Contact: B. W. Sheron, NRR, X27588

Enclosure (1)

Summary

The inspection plan was to audit two thermal-hydraulic safety analysis computer codes, one transient and one ECCS. These were selected as the LOFTRAN and LOCTA codes respectively.

The procedures for thermal-hydraulic safety analysis code control were recently issued and were not the ones in effect when the codes were originally developed.

In addition to the departmental procedures, Westinghouse also has divisional procedures for each division, which are called division standards. These documents however, appeared to be more specification documents on how to use the safety analysis codes within that division.

No discussions with Westinghouse staff engineers on quality control practices for code use were held due to time limitations.

Enclosure (2) provides discussions of our observations regarding their procadures. These observations were provided to Westinghouse management at the exit interview of the inspection. Some additional discussion however, has been provided to better clarify the observations.

Enclosure (2)

A. General Observations

1. Procedures do not address how errors identified in NRC-reviewed codes are reported to NRC. Westinghouse stated that only those errors in non-LOCA codes which would affect technical specification limits are considered reportable. No procedures exist for reporting violations of Appendix K to 10CFR50.

2. Warning statements regarding recommended restrictions on code applicability were found in design record file documentation. There was no indication that followup action was taken to either resolve the concern or to formally restrict use of the code. It was unclear if licensing analyses were affected by these use restrictions.

3. Some microfische records were not legible. These records were not the design record file however.

4. It is not clear which codes should constitute the LOCA ECCS evaluation model and which should not, with particular reference to ancillary codes used for input data manipulation/preparation. While it was acknowledged that the codes which comprise the ECCS model were agreed upon previously with NRC, it was noted that a code used to calculate the steam generator initial enthalpy

distribution, called HMSGPD, could be construed as part of the model per the requirements of 10CFR50.46(C)(2). Westinghouse did not consider it part of the model however.

5. Use of only a design review is not considered as either independent or adequate verification for safety analysis computer code development or modification. Design review in this case means a review by an individual or committee that does not include the performance of alternate calculations, comparisons to data, etc. by that individual or committee.

   Westinghouse documents work performed on code modification or development on "calcnotes". This is a standardized form which is given a division document number for each calcnote, and provides for an originator and reviewer's signature. The reviewer is considered the verifier, in that his review of a calcnote is considered verification by "design review". Actual verification work is usually performed by the originator.

6. During the review of the calcnotes for the Zirconium-Water error correction, it was noted that other modifications were made to the LOCTA code which affected the LOCTA-calculated PCT by 24°F. No followup calculations of the effect on a complete ECCS calculation were performed nor were the model changes identified in WCAP 9220. It was noted, however, that the model change and modifications were made as part of a more thorough review of the LOCTA code after the Zirconium-Water error was found.

7. The meaning of independent verification is not clearly identified on the Computer Program Change Request Form. This form contains spaces for an originator and verifier to sign. This however, does not refer to verification of the technical work, but only assurance of successful updating of a computer tape. This was confusing, since for tape updating, the originator is normally the verifier, and therefore the same name would appear on both parts of the Change Request Form.

8. Westinghouse does not consider more QA procedures to be cost effective for uncovering code errors.

9. Westinghouse procedures do not require the reexamination and re-evaluation of procedures in the event of code errors. This does not mean a re-evaluation that determines it is not appropriate to re-evaluate procedures. Westinghouse stated that after the discovery of the Zirconium-Water reaction error, they determined that it was not a fault of the procedures and therefore did not reexamine the procedures.

10. Other codes referenced in computer program documents are not described or referenced adequately.

    In reviewing the LOFTRAN document, reference was made to the FRED code. No reference nor even a brief description was provided of this code. For reviewers outside of Westinghouse, this could present difficulties in the review.

11. No requirements exist for the correction of errors in WCAPs. Documentation was found which discussed errors in a WCAP report. No procedures exist which assure that these errors are corrected in a timely manner, especially for those reports submitted in support of licensing action.

12. Code input options do not appear to be sufficiently identified in the Safety Analysis Standards document. Westinghouse has internal documents called Division Standards. These documents contain procedures one step removed from OPR procedures and are primarily related to details of code use. Little information on either code input options available, or model options available in the code was found in the Division Standards.

13. New versions of codes are not regularly compared against available data that earlier versions of the code have been compared against.

    This information could contribute significantly to verification efforts, yet it appears such comparisons are not frequently performed.

14. Std. #19 of the Safety Analysis Standard references an out-of-date version of the topical for LOFTRAN

15. Standards have not been revised to correct deficiencies known to exist (in some cases the corrections have been penned in). These standards appear to constitute a major part of the code

use information, yet they are not controlled documents and provide no means of assuring they are kept up to date.

16. Appendix A of procedure OPR-WRD-300-1 discusses verification of a computer code and verification of the application of a computer code. The latter is also referred to as qualification. It was not clear what the distinction is between these two.

17. Calcnote forms do not require the verifier to document what was done to verify the material in the calcnote, only a signature is necessary.

B. <u>Code Deficiencies</u>

1. <u>Zirconium-Water Reaction Rate Error</u>

The error in Zirconium-water reaction rate was discovered by Framatone Company in France, which has a licensing agreement with Westinghouse. In the course of performing errant pellet analyses (mixed enrichment with one pellet at a higher enrichment than others) they noted the Zirconium-water reaction rate was not as high as expected on the higher enrichment pellet. Framatone followed up with heat balance checks and concluded the error was in the Zirconium-water reaction rate calculation. They notified Westinghouse, who confirmed the error, and the Westinghouse Safety committee was immediately informed. The sequence of dates was:

<u>March 14th, 1978</u> Framatone sends Westinghouse a Telex of suspected error

March 22nd, 1978 Westinghouse confirms error

March 24th, 1978 Brought before Safety Committee, determined in violation of Appendix K, and NRC was immediately notified.

As a result of the error, Westinghouse reviewed the whole subroutine in which the error was found. This lead them to make other modifications to the code.

The error was apparently put in the code during the 1974 EM model approvals, and Westinghouse feels that rush to get an approved EM model at that time probably caused the error.

2. Upper Head Temperature

This error was also introduced in 1974. The pressure distribution in upper head was assumed uniform and was assumed to be at the cold leg temperature.

Subsequent 1/7 scale tests showed there was a radial pressure gradient in upper plenum. The result of this was that fluid could flow from the upper plenum to the upper head, which was contrary to the initial assumption. Westinghouse found a plant, Connecticutt Yankee, with 8 thermocouples in the upper head. This data showed the upper head temperature at about 70% of the way to T_{hot} from T_{cold}.

Westinghouse performed more analyses, and looked for more plant data. The issue was taken to the safety Committee, which concluded that it was a violation of Appendix K, plus an unreviewed safety issue.

The whole process took about 3-4 months from the time it was first thought to be a problem to the time it was reported.

Westinghouse also undertook an upper head temperature test program. These results also showed the upper head temperature was somewhere between T_{hot} and T_{cold}.

Westinghouse stated that they did examine the model to see if there were other places wrong input might be possible, but none were discovered.

3. LOFTRAN

The LOFTRAN error was that a safety valve flow was not included in the calculation of total steam flow.

The cognizant engineer stated that this was due to a misplaced card in the program, and was not considered to be the type of mistake that better procedures would have caught. The error was found by discrepancies noted between the LOFTRAN calculation and a similar calculation performed with a different code.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

NOV 27 1978

MEMORANDUM FOR: Z. R. Rosztoczy, Chief, Analysis Branch, DSS

FROM: B. W. Sheron, Analysis Branch

THRU: L. E. Phillips, Section Leader, Analysis Branch, DSS LEP

SUBJECT: TRIP REPORT: INSPECTION OF COMBUSTION ENGINEERING QA CONTROLS FOR SAFETY ANALYSIS CODE DEVELOPMENT

Enclosure (1) documents the report of the trip which Paul Norian, Norm Lauben and I took to Combustion Engineering on November 14-16, 1978. The purpose of this trip was to accompany the Region IV inspector (D. Anderson) on his inspection of CE's QA controls for Safety Analysis Code Development in the thermal-hydraulic area.

The observations reported in Enclosure (1) are consistant with the inspection report. While these observations may imply recommended changes to the procedures, it is not the intent of this report to put forth such recommendations. The final report documenting the results of the entire review will present any recommendations and conclusions.

Brian W Sheron
Brian W. Sheron
Analysis Branch
Division of Systems Safety

Enclosure:
As stated

cc: R. Mattson PDR
R. Tedesco
T. Novak
K. Kniel
R. Brickley, Region IV
D. Anderson, Region IV
C. Hale, Region IV
W. Rutherford, IE
A. Bates, ACRS
W. Lyon, RES
W. Haass, OPM
J. Gilray, OPM
S. Hanauer, EDO
P. Norian
G. N. Lauben

Contact: NRR:B. Sheron, Ext. 27588

1.0 Introduction

On November 14-16, 1978, P. Norian, G. N. Lauben, and B. Sheron accompanied D. Anderson of Region IV on an inspection of CE's QA controls for safety analysis code development in the thermal-hydraulic area.

The two computer codes inspected were the STRIKIN-II ECCS code and the CESEC transient analysis code.

STRIKIN-II is used to calculate the peak cladding temperature and local clad oxidation throughout the LOCA analysis. CESEC is used to calculate the system thermal-hydraulic transients.

In late 1975 through 1976, CE performed audits on the STRIKIN-II and CEFLASH codes. As a result of these audits, a number of errors found in the STRIKIN code were reported. Since these have been the only errors reported by CE to date, since they were all discovered as a result of the audit, and since they all got in the code during the evaluation model approval period of 1974, no separate review of previous code errors, how they were discovered, etc. was conducted similar to reviews conducted during other vendor inspections.

2.0 Areas for Consideration by Combustion Engineering

The following 14 items were identified at the end of the inspection to the Combustion Engineering management for consideration and are documented as follows:

1. There does not appear to be any central index to define what constitutes the code design file, or a project design file.

2. Procedures do not address how modifications to NRC-approved codes are reported to NRC.
3. The "ECCS Licensing Analysis Verification Checklist" was found in the System 80 CEFLASH calculational input file, but not in other files. We encourage the use of such a checklist for all calculations and its inclusion in the design files.
4. There appears to be no information in the ECCS code files regarding verification by comparison to test data. Such comparisons are available through programs such as the standard problem program. We believe this form of verification to be applicable to parts of evaluation model codes and should be included in the code verification files.
5. On the ECCS Licensing Analysis Verification Checklist, item 25 was checked "yes", indicating experimental data were employed. No evidence of how the experimental data were employed was found.
6. Procedures do not address how errors identified in codes are dispositioned.
7. A chronological listing of development, review, approval and changes to codes had not been documented.
8. Procedures do not exist for detailing the process to be followed when existing codes are used in applications other than those for which the code was originally developed.
9. Documentation of comparison of codes with previous results is not being maintained.
10. Documentation of the review of QA Folders for [illegible]es is not being maintained.

11. Documentation is not being maintained which addresses why a change to a code is being made.

12. Departmental level procedures for code development, review, approval, and control do not exist.

13. CESSAR/FSAR/System 80 LOCA Analyses were submitted to NRC prior to the completion of independent review of the analyses. QA review and verification of all documents should be completed prior to submittal to NRC.

14. Procedures do not address how individual codes are to be used in an overall analysis model or package. Also, there are no requirements for assuring that integral results developed from more than one code are independently reviewed.

3.0 Other Observations

3.1 In 1976, CE performed an internal QA audit of the STRIKIN ECCS code. This was done at the time the QADM (Quality Assurance Design Manual) was first issued. Prior to issuance. of the QADM, no formal code "control" procedures were in existance.

3.2 CE procedures make clear that independent verification is not required, only independent review of verification. Verification (i.e., alternate calculations, etc.) is normally performed by the developer and independently reviewed. The detailed documentation required by CE provides a traceable description of verification methods, and documents the extent of the independent review.

3.3 An ECCS calculational flow chart showing all of the codes used in an ECCS calculation indicated a number of utility codes used. CE defines utility codes as "minor codes which automate hand calculations or perform simple data processing manipulations". (5.2.4.1 of QADP 5.2). Based on 10 CFR 50.46 (c) (2) (definition of evaluation model) these utility codes are part of the ECCS model. CE considers them as part of the model, and stated that they undergo the same QA as the big ECCS codes, have the same certification, etc.

The notebook for the CEFLASH-4A system 80 Large Break analyses provided a well-documented trail of input data derivation such that it could be traced without recourse to the originator. The notebook also contained a signed and dated checklist by the reviewer, as well as an analysis cover sheet signed and dated by the author and reviewer.

3.4 For the System 80 calculational file, the results were checked according to the documentation, which implies they were checked against the ECCS Licensing Analysis Verification checklist. This is not clear, and in no instance was any documentation found in which the method of checking the output (results) was described.

3.5 There appears to be no information in the ECCS code files regarding verification by comparison to tests. CE participates in the standard problem program and therefore such comparisons are available. The results and conclusions from such comparisons should be incorporated in the code design file.

CE does not believe the results of such comparisons are applicable to the EM version of the code, since the EM version is approved and therefore no further verification is needed. As such, no comparisons of integral systems data are considered applicable for verification, and therefore not used or contained in the code design file. This appears to be another area in which the verification method of comparison to data in ANSI N.45.2.11 is inapplicable to Licensing code development. CE did state that the experiments run for the standard problem program do help them in developing best-estimate codes.

3.6 CE stated that the present QA procedures were not in effect at the time the code audit was performed, and therefore notebooks documenting the checkout of the code corrections are not available. An internal letter which describes the errors and how they were corrected was written. CE stated that independent reviews, etc... were performed for these changes.

3.7 Most of the System 80 FSAR ECCS calculational notebooks, which document the derivation of inputs, were not signed by the independent reviewer, although the FSAR had already been submitted. CE stated that these were not signed because all of the input received from engineering had not been verified by Engineering as final. As such, there was no evidence that the System 80 FSAR ECCS analyses had any sort of verification performed prior to their submittal to NRC.

APPENDIX B

OFFICE OF INSPECTION AND ENFORCEMENT

REGION IV INSPECTION REPORTS

UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION IV
611 RYAN PLAZA DRIVE, SUITE 1000
ARLINGTON, TEXAS 76011

THIS DOCUMENT HAS NOT BEEN REVIEWED FOR PROPRIETARY INFORMATION AS DESCRIBED IN 10 CFR 2.790
B.U.Sheron-Hyo

22 NOV 1978

Docket No. 99900081/78-03

Exxon Nuclear Company
ATTN: Mr. G. F. Owsley
Manager, Reload Licensing
2101 Horn Rapids Road
Richland, Washington 99352

Gentlemen:

This refers to the QA Program Inspection conducted by Mr. D. G. Anderson of this office on October 30 - November 3, 1978, of your facility at Richland, Washington, and to the discussions of our findings with you and members of your staff at the conclusion of the inspection.

Areas examined during the QA Program inspection and our findings are discussed in the enclosed report. Within these areas, the inspection consisted of an examination of procedures and representative records, interviews with personnel, and observations by the inspector.

During this inspection it was found that the implementation of your Quality Assurance Program failed to meet certain NRC requirements. The specific findings and references to the pertinent requirements are identified in the enclosures to this letter.

Please provide us within thirty (30) days a written statement containing, (1) a description of any steps that have been or will be taken to correct this item, (2) a description of any steps that have been or will be taken to prevent recurrence, and (3) the dates your corrective actions and preventive measures were or will be completed.

In accordance with Section 2.790 of the Commission's "Rules of Practice," Part 2, Title 10, Code of Federal Regulations, a copy of this letter and your reply together with the enclosed inspection report will be placed in the Commission's Public Document Room. If this report contains any information that you believe to be proprietary, it is necessary that you make a written application within thirty (30) days to this office to withhold such information from public disclosure. Any such application must include a full statement of the reasons on the basis of which it is claimed that the information is proprietary, and should be prepared so that proprietary information identified in the application is contained in a separate part of the document. If we do not hear from you in this regard within the specified period, the report will be placed in the Public Document Room.

Should you have any questions concerning this inspection, we will be pleased to discuss them with you.

Sincerely,

Uldis Potapovs, Chief
Vendor Inspection Branch

Attachment:
1. Notice of Deviation
2. Inspection Report No. 99900081/78-03

bcc:
AD/RCI (REINMUTH)
E FILES
NRR:DPM:QAB
REG. I, II, III, & V
PDR HQS
CENTRAL FILES
WEVETTER, RIV

Exxon Nuclear Company
Docket No. 99900081/78-03

NOTICE OF DEVIATION

Based on the results of an NRC inspection conducted on October 30 - November 3, 1978, it appeared that certain of your activities were not conducted in full compliance with NRC requirements as indicated below:

Criterion V (Instructions, Procedures, and Drawings) of Appendix B to 10 CFR Part 50 states in part, "Activities affecting quality shall be prescribed . . . and shall be accomplished in accordance with these instructions, procedures, or drawings." The corresponding applicable Section 3.0, Design Control, of the Exxon Topical Report, XN-NF-1, states in part that "The Preparation of design documents are performed in accordance with approved procedures . . . ."

Contrary to the above, certain activities were not prescribed by or accomplished in accordance with approved procedures:

1. Procedures do not exist describing the method by which changes to the evaluation model are reported in amendments submitted to the NRC as required by paragraph 1.b. of Section II of 10 CFR 50, Appendix K.

2. In two cases, calculation forms had not been completed and calculation indexes had not been prepared as required by Procedure XN-NF-500, 002, Section 6.0, Design Process.

VENDOR INSPECTION REPORT

U. S. NUCLEAR REGULATORY COMMISSION
OFFICE OF INSPECTION AND ENFORCEMENT
REGION IV

Report No. 99900081/78-03 Program No. 44010

Company: Exxon Nuclear Company
2101 Horn Rapids Road
Richland, Washington 99352

Inspection Conducted: October 30 - November 3, 1978

Inspectors: R. H. Brickley 11/16/78
for D. G. Anderson, Principal Inspector, Vendor Inspection Branch — Date

Other Personnel: R. H. Brickley 11/16/78
for B. W. Sheron, Nuclear Engineer, DSS/NRR — Date

R. H. Brickley 11/16/78
for R. F. Audene, Nuclear Engineer, DSS/NRR — Date

R. H. Brickley 11/16/78
for P. E. Norian, Section Leader, DSS/NRR — Date

Approved by: R. H. Brickley 11/16/78
for C. J. Hale, Chief, Vendor Program Evaluation Section, Vendor Inspection Branch — Date

Summary

Special Inspection conducted on October 30 - November 3, 1978 (99900081/78-03)

Areas Inspected: 10 CFR 50, Appendix B, and Topical Report XN-NF-1 as applied to the establishment and implementation of procedures to control

the development and revision of safety analysis computer codes. The inspection involved thirty (30) inspector hours on site by one (1) USNRC Region IV inspector.

Results: In the area inspected there were no unresolved items and one (1) deviation with two (2) examples identified as follows:

Deviation: 10 CFR 50, Appendix B, Criterion V, and Section 3.0 of Topical Report XN-NF-1-procedures do not exist for the evaluation and reporting of significant changes in the evaluation model as referenced in Criterion II.b. of 10 CFR 50, Appendix K. (See Notice of Deviation, Enclosure, Example 1.) Calculation Forms were not completed and Calculation Indexes were not prepared as required by procedure XN-NF-500, 002 (See Notice of Deviation, Enclosure, Example 2).

DETAILS SECTION

(Prepared by D. G. Anderson)

A. Persons Contacted

*R. E. Collingham, Manager, System Model Development
*G. C. Cooke, Manager, Fuel Response Analysis
*M. S. Foster, Manager, EDP Programming
*K. P. Galbraith, Manager, Nuclear Safety Engineering
*S. E. Jensen, Manager, Systems Analysis
*D. C. Kolesar, Engineer
*G. F. Owsley, Manager, Reload Licensing
*D. K. Perry, Quality Assurance Engineer
*J. A. Perry, Manager, Quality Assurance

*Denotes those present at the exit meeting.

B. Introduction

This report covers a special inspection conducted to examine the establishment and implementation of procedure controlling safety analysis computer code development. The objectives of this inspection are:

1. To determine that adequate procedures to minimize the potential for analysis errors to go undetected have been established for control of the development and revision of these codes.

2. To determine that these procedures were fully implemented during the development and revision of selected codes.

C. Control of Safety Analysis Computer Codes

1. Establishment of Procedures

a. Inspection

(1) The Exxon Nuclear Company Topical Report, XN-NF-1, requires in Section 3.0, Design Control, that "Design of fuel assemblies and related components and the preparation of design documents are performed in accordance with approved procedure and techniques." Section 3.5 states that "The adequacy of product designs may be verified in several ways, including in reactor experience of similar design performance

of design reviews, alternate calculations, or design testing." These commitments are implemented by the following Exxon Nuclear Company procedure:

XN-NF-500, 002, Fuel Design and Engineering Quality Assurance Procedures for Fuel Fabrication - Product Line and Related Components.

(2) An examination of XN-NF-500, 002, revealed that there are requirements for testing, documentation, verification, and control of computer programs. The verification documentation is required to be maintained in a design file at the Control Files location. Section 6.9.2 identifies those records to be included in the design file. A Computer Code Council is responsible for the administrative and quality assurance aspects of Exxon Nuclear Computer programs and programming.

This procedure also details the requirements for development of ECCS Computer programs and the modification of existing computer programs are established along with the definition of responsibilities of individuals in the verification chain.

b. Findings

The procedure used to implement Exxon Topical Report, XN-NF-1 appears to meet the requirements of ANSI N45.2.11 as appropriate to verification, and documentation of this verification for Safety Analyses Computer Codes. During the examination of this implementing procedure and the documentation generated as a result of following the procedure, the following items were identified and Exxon Management indicated that they would consider further action, as appropriate. Any action taken by Exxon will be examined during a future inspection.

(1) There are no formal procedures for the documentation, timely assessment, and resolution of potential safety concerns, nor are there any procedures for reporting ECCS model changes per the requirements of 10 CFR 50, Appendix K.

(2) There are no procedures considered by Exxon to be applicable to code development. Existing procedures are only considered applicable to code use.

(3) Verification information should be documented in the project files. Exxon also stated that Management signatures on topical report constituted verification by design review. We do not believe this to be an acceptable method of verification.

(4) When changes are made to the code, letters to code users informing them of the changes should be issued and included in the code file. When code versions are approved, the approval letters should be kept in code file.

(5) In some instances, signatures indicating that independent checks were performed on final calculations were not found.

(6) It was found in some cases that input data calculations were dated after the ECCS analyses were completed and the topical report approved by Exxon Management and submitted to NRC. Independent checks were dated as much as 3 months after Management approval. This item was identified by Exxon in an Internal Audit. Corrective Action has been initiated.

(7) There is no procedure which requires input data, as it is put into the code, to be independently checked.

(8) Exxon should have procedures specific to how codes developed by Exxon contractors are to be checked out and verified by Exxon. These procedures should be more specific than those that presently exist in the area of verification requirements.

(9) Procedures do not exist which describe the detailed preparation, development, review, approval, and control of computer codes.

(10) Procedures should address the details of preparation, completion, checking, signing, identification, indexing, etc., for calculation forms which are used in code development.

(11) Procedures do not address how errors are identified, corrected, or flagged in master codes.

(12) The categorization of codes into 3 classes; master, developmental, and special, does not appear to be sufficient to assure protection of NRC-approved codes.

More specific categorization which provides better protection of NRC-approved codes against unauthorized modification is recommended.

(13) There is no evidence that code design and project files are indexed, nor is there any requirement that they be indexed. Without indexing, there is no record of what documents constitute a code design or project files.

(14) Definitions in procedure XN-NF-500, 002 should be more extensive, encompassing such items as verification, qualification, etc...

(15) In some instances, calculational files are only signed by the checker on the first page. This signature is intended to indicate that all pages of the calculation were checked. Better confidence that all pages were checked would be obtained if (1) all pages were signed, and (2) the checker documented in a brief statement the extent and scope of the check.

2. Implementation of Procedures

a. Inspection

The development and revision of the following computer programs was evaluated for meeting the requirements of procedure XN-NF-500, 002 related to verification and control:

WREM: The base for the Exxon Nuclear Company PWR generic water reactor evaluation model. The PWR evaluation model includes RELAP-4 EM, RELAP-4 FLOOD and TOODEE 2. RELAP-4 EM computes the space and time variation of the thermal-hydraulic conditions of the primary and secondary systems during the decompression of the primary system following a LOCA. RELAP-4 FLOOD is used to calculate the reflooding rates starting at the beginning of core recovery. TOODEE 2 calculates the hot fuel rod temperature analysis from bottom of core recovery through the reflood period until core quench.

PTSBWR 2: A digital computer program, written in Fortran language, which simulates the behavior of non-jet pump BWR's under irregular operating condition such as steamline isolations, coolant recirculation malfunctions and feedwater malfunctions. Calculates fluid conditions, flow rates, heat flux, reactor power and reactivity as a function of time.

The inspector examined the documentation contained in the design file on these two (2) computer programs which consisted of eight (8) memoranda transmitted between Exxon and Service Computer organizations, sixteen (16) internal memoranda related to computer code changes, seven (7) computer code Topical Reports contained in Exxon documents, twenty-nine (29) calcuation forms related to verification of computer programs, seven (7) meeting minutes of the Computer Code Council, one (1) internal audit of the Computer Code Council, twenty (20) Standard Sample Problem Verification Forms, fifteen (15) verification indexes, five (5) Master Computer Code Approval Forms, one (1) Computer Code Masterization Procedure Checklist, two (2) Master Code listings, two (2) telephone memoranda related to questions from Service Computer organizations about computer code use, and nine (9) computer code runs related to code verification.

b. Findings

In this area of the inspection, no unresolved items were identified. One (1) deviation from commitment with two (2) examples was identified (See Notice of Deviation, Enclosure).

D. Exit Meeting

An exit meeting was conducted with management representatives at the conclusion of the inspection on November 3, 1978. Those individuals indicated by an asterisk in Section A of the Details Section of this report were in attendance.

The inspector discussed the special nature of this inspection and the scope and finding indentified during this inspection. Management representatives of Exxon acknowledged the statments by the inspector with respect to the one (1) deviation presented.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION IV
611 RYAN PLAZA DRIVE, SUITE 1000
ARLINGTON, TEXAS 76011

THIS DOCUMENT HAS NOT BEEN REVIEWED FOR PROPRIETARY INFORMATION AS DESCRIBED IN 10 CFR 2.790
B.W. Sheron
AB, NRR-Hq

SEP 15 1978

Docket No. 99900400/78-03

The Babcock & Wilcox Company
Nuclear Power Generation Division
ATTN: Mr. J. H. MacMillan
Vice President
Post Office Box 1260
Lynchburg, Virginia 24505

Gentlemen:

This refers to the QA Program Inspection conducted by Mr. R. H. Brickley, of this office on August 29-31, 1978, of your facility at Lynchburg, Virginia, and to the discussions of our findings with you and members of your staff at the conclusion of the inspection.

Areas examined during the QA program inspection and our findings are discussed in the enclosed report. Within these areas, the inspection consisted of an examination of procedures and representative records, interviews with personnel, and observations by the inspector.

During this inspection it was found that the implementation of your QA program failed to meet certain commitments in your Topical Report No. BAW-10096A. The specific findings and references to the pertinent requirements are identified in the enclosures to this letter.

Please provide us within thirty (30) days a written statement containing, (1) a description of steps that have been or will be taken to correct this item, (2) a description of steps that have been or will be taken to prevent recurrence, and (3) the dates your corrective actions and preventive measures were or will be completed.

In accordance with Section 2.790 of the Commission's "Rules of Practice," Part 2, Title 10, Code of Federal Regulations, a copy of this letter with enclosure and your reply together with the enclosed inspection report will be placed in the Commission's Public Document Room. If this report contains any information that you believe to be proprietary, it is necessary that you make a written application within thirty (30) days to this office to withhold such information from public disclosure. Any such application must include a full statement of the reasons on the basis of which it is claimed that the information is proprietary, and should be prepared so that proprietary information identified in the application is contained in a separate part of the document. If we do not hear from you in this regard within the specified period, the report will be placed in the Public Document Room.

Should you have any questions concerning this inspection, we will be pleased to discuss them with you.

Sincerely,

Uldis Potapovs

Uldis Potapovs, Chief
Vendor Inspection Branch

Enclosures:
1. Notice of Deviation
2. Inspection Report No. 99900400/78-03

bcc:
AD/RCI (REINMUTH)
IE FILES
NRR:DPM:QAB
REG. I, II, III, & V
PDR HQS
CENTRAL FILES
WEVETTER, RIV

The Babcock & Wilcox Company
Nuclear Power Generation Division
Docket No. 99900400/78-03

NOTICE OF DEVIATION

Based on the results of an NRC inspection conducted on August 29-31, 1978, it appears that certain of your activities were not conducted in full compliance with NRC requirements as indicated below:

Criterion V (Instructions, Procedures, and Drawings) of Appendix B to 10 CFR 50 and the corresponding Section 5 of the Babcock & Wilcox topical report BAW-10096A (B&W NPGD Quality Assurance Program For Nuclear Equipment) state that activities affecting quality shall be prescribed by documented instructions, procedures, or drawings, of a type appropriate to the circumstances and accomplished accordingly. Section 5 of BAW-10096A further states that these procedures are implemented by publication in the NPGD Administrative Manuals.

Contrary to the above, certain activities were not accomplished in accordance with your procedures as follows:

1. Step 11 of Exhibit B (Certification of Computer Programs) to published procedure NPG-0902-06 (Computer Program Development and Certification) states in part, ". . . File original documentation in certification files." Further Step 1 defines a typical program package to consist of the request, program, and program manual.

   Contrary to the above, the original documentation for the Conditional Certifications for Version 4 of TRAP2 issued January 24, 1978, and Version 4.1 of TRAP2 issued February 9, 1978, were not filed in the Certification Files for the TRAP program.

2. Step 12 of Exhibit B to NPG-0902-06 states in part, ". . . Initiate Program Abstract and insert in NPGD-TM-338."

   Contrary to the above, the Program Abstract for Conditional Certification of Version 3 of TRAP2 issued on December 20, 1977; Version 18 of TRAP issued on March 3, 1978, and Version 4.1 of TRAP2 issued on February 9, 1978, were not inserted in NPGD-TM-338.

3. Section IV (Program Abstract) of NPG-0902-06 states in part, ". . . This (Program Abstract) is a computerized format . . . that describes certain aspects of the program (i.e. . . . Responsible Engineer and Programmer, ..."

   Contrary to the above, the latest revision (14) to NPGD-TM-338 does not describe (identify) the Responsible Engineer and Programmer.

Results: In the area inspected there were no unresolved items and one deviation identified as follows:

Deviation: 10 CFR 50, Appendix B, Criterion V and Section 5 of Topical Report BAW-10096A - three (3) examples of a failure to follow procedures in the development and revision of safety analysis computer codes. (See Notice of Deviation enclosure.)

VENDOR INSPECTION REPORT

U. S. NUCLEAR REGULATORY COMMISSION
OFFICE OF INSPECTION AND ENFORCEMENT
REGION IV

Report No. 99900400/78-03 Program No. 44081

Company: The Babcock & Wilcox Company
Nuclear Power Generation Division
Post Office Box 1260
Lynchburg, Virginia 24505

Inspection Conducted: August 29-31, 1978

Inspector: R. H. Brickley 9/8/78
R. H. Brickley, Principal Inspector, Vendor Inspection Branch — Date

Other Personnel: for R. H. Brickley 9/8/78
Z. R. Rosztoczy, Chief, Analysis Branch, NRR — Date

for R. H. Brickley 9/8/78
B. W. Sheron, Nuclear Engineer, AB/NRR — Date

for R. H. Brickley 9/8/78
J. W. Gilray, Section Chief, QAB/NRR — Date

Approved by: C. J. Hale 9-12-78
C. J. Hale, Chief, Projects Section, Vendor Inspection Branch — Date

Summary

Special Inspection conducted on August 29-31, 1978, (99900400/78-03)

Areas Inspected: 10 CFR 50, Appendix B and Topical Report BAW-10096A as applied to the establishment and implementation of procedures to control the development and revision of safety analysis computer codes. The inspection involved twenty-four (24) inspector hours on site by one NRC Region IV inspector.

DETAILS

A. Persons Contacted

*J. J. Cudlin, Manager, LOCA Methods Unit
*B. M. Dunn, Manager, ECCS Analysis Unit
*D. W. La Belle, Manager, Safety Analysis Unit
*C. D. Morgan, Manager, Technical Staff
K. C. Shieh, Principal Engineer, ECCS

*Denotes those present at the exit interview.

B. Introduction

This report covers a special inspection conducted to examine the establishment and implementation of procedures controlling safety analysis computer code development. The objectives of this inspection are:

1. To determine that adequate procedures to minimize the potential for analysis errors to go undetected have been established for control of the development and revision of these codes.

2. To determine that these procedures wer fully implemented during the development and revision of selected codes.

C. Control of Safety Analysis Computer Codes

1. Establishment of Procedures

a. Inspection

An examination of the Nuclear Power Generation Division (NPGD) Administrative Manual, which contains procedures implementing topical report BAW-10096A (B&W NPGD Quality Assurance Program for Nuclear Equipment), revealed that procedure NPG-0902-06 (Computer Program Development and Certification) is the principal document governing this activity. Procedure NPG-0903-03 (Internally Developed Computer Program Manuals) governs the preparation and issuance of the "user" manual.

The examination of procedure NPG-0902-06, Revision 1 dated January 26, 1978, revealed that it requires certification of all computer codes, except those not used for contract work, employed in the performance of calculations for non-safety related items consisting of 100 or less Fortran statements, prepared and used prior to September 28, 1973, but no longer employed at the performance of design verification calculations, and nonproduction computer programs that do not solve a mathematical equation. However, the procedure requires that the programs not subject to certification be independently reviewed and documented in accordance with their intended application. There are four (4) levels of certification required: Full Certification, Conditional Certification, Prior Certification and Interim Use. Full Certification applies to programs which have been subjected to careful examination for programming and modeling accuracy, to verification of results using analytical and/or experimental data and to production testing (execution of sampling cases which typify production usage) prior to use. Conditional Certification applies to new programs or modified versions of production programs, when the new or modified program must be released for production work prior to the completion of the full certification process. Prior Certification applies to programs which have been superseded by new or revised programs but which must be retained for further analysis on those contracts where analyses are in progress or have been completed. Interim Use applies to all programs which have been submitted for use but for which verification/documentation only exists in contract records. Computer programs which are verified and certified for contract use are identified as production programs. These programs are jointly developed and documented by Computer Services and Technical Staff and are programs approved for use. Exhibit A of this procedure is a flow diagram identifying, by title, the individuals involved in computer program development and the requirements for each step of the process. Exhibit B of this procedure is a flow diagram identifying, by title, the individuals involved in computer program certification and the requirements for each step of the process.

The examination of procedure NPG-0903-03, Revision 3, dated May 2, 1977, revealed that fully certified computer programs are required to have a Program Manual when they are released for use. Those programs released with a conditional certification are required to have a Conditional Program Manual defined as consisting of a Program Abstract, input instructions, and output information.

b. Findings

During the examination of the B&W administrative procedures the following items were identified and B&W management stated they would consider further action, as appropriate. Any action taken by B&W will be examined during a future inspection.

(1) Procedure NPG-0902-06 does not require a specific time limit on how long a computer program can remain in a conditional certification status before it must undergo the full certification process.

(2) Procedure NPG-0902-06 does not appear to specify a method for termination of a version of a code which is found to contain an error and/or has been superceded by a new version.

(3) Procedure NPG-0902-06 does not require that users of a code, that subsequently was found to contain an error, be notified of the error and requested to evaluate its effect on past analysis. In addition, the procedure does not require that the corrective actions taken to correct an error found in one version of a code be applied to other versions.

(4) Procedure NPG-0903-03 does not require that the computer program manual be a controlled document similar to the B&W Administrative Manual even though these manuals are used in safety analysis work.

(5) Procedure NPG-0902-06 does not specify a method that provides traceability between Form PDS-21177 (Computer Program Certification), Form PDS-21126 (Request for Programming Services), Program, and Program Manual (Revision) submitted for Full and Conditional Certification.

(6) Procedure NPG-0902-06 does not specifically define the revision/version notation of the computer programs, i.e. Is it Version A of TRAP1 or Version 1A of TRAP; Version 2 of TRAP or Version 0 of TRAP2, etc.

(7) Step 8 of Exhibit 3 to NPG-0902-06 states that the "Technical Staff Engineer" (B&W representatives stated that this meant Technical Staff Manager) "Assign Technical Staff Engineer to evaluate the program." Since a Technical Staff Engineer can initiate the request for certification it is not clear that the same person can perform this evaluation.

(8) There appears to be some confusion as to the extent of the applicability of procedure NPG-0402-01 (Processing of NPGD Prepared Calculations) with respect to the independent verification review and documentation of the development, revision, and certification of computer program.

(9) Procedure NPG-0902-06 does not require the documentation of evaluations when detected program errors are determined not to have any safety significance.

2. Implementation of Procedures

a. Inspection

The development and revision of the B&W computer program TRAP (Transient Reactor Analysis Program) was selected by AB/NRR personnel for examination. The inspector examined the official files maintained on this program i.e. twenty-five (25) IOMs, ten (10) Form PDS-21186 (Request for Programming Services), eighteen (18) Form PDS-21177 (Computer Program Certification), program manual NPGD-TM-414 (TRAP2-FORTRAN Program for Digital Simulation of the Transient Behavior of the Once-Through Steam Generator and Associated Reactor Coolant System), and NPGD-TM-338 (Computer Program Abstracts).

b. Findings

(1) The IOMs examined covered a variety of subjects concerning the TRAP program e.g. Basis for Conditional Release of TRAP dated September 27, 1973; Conditional QA for TRAP dated April 26, 1974; TRAP Digital Simulation Comparison with Oconnee 1 Transient Data, May 6, 1975; Problems with TRAP 2 dated November 25, 1975; Change needed in TRAP 1B dated June 28, 1976; Request for TRAP 2 Code Modification dated March 30, 1977; Errors in TRAP 1 & 2 dated January 12, 1978; etc.

(2) The forms PDS-21186 that were examined are part of a package (Request, Program, and Program Manual) submitted for Full and Conditional Certification. This form requires a statement of the Program Parameters/Specification which shall contain a general description of the calculation to be evaluated, the actual equations and a suggested solution technique (if known), a description of the necessary program input and output, and sample test data sufficient to test the options requested (Section V of NPG-0902-06).

(3) The Forms PDS-21177 that were examined were for the Conditional Certification of various versions of the TRAP code i.e. Version 1 of TRAP, Version 1A of TRAP, Version 1B of TRAP, Version 2 of TRAP, Version 3 of TRAP 2, Version 3.2 of TRAP 2, Version 4 of TRAP 2, and Version 4.1 of TRAP 2. Some of these versions had their Conditional Certification reissued several times.

(4) Three (3) examples of a single deviation were identified. (See Notice of Deviation).

D. Exit Interview

An exit interview was held with anagement representatives on August 31, 1978. In addition to those ind .iduals indicated by an asterick in paragraph A, those in attendance were:

J. D. Agar, Manager, Contract Licensing
C. A. Armontrout, Lead QA Engineer
L. L. Barinka, Manager, Applied Mathematics Unit
P. N. Calpo, Manager, Engineering Applications Program Unit
A. L. MacKinney, Manager, QA Department
J. H. MacMillan, Vice President
P. J. Motiska, Principal QA Engineer
W. E. Patscheider, QA Engineer
D. H. Roy, Manager, Engineering Department
R. H. Standt, Manager, Thermodynamics Unit
B. W. Whitaker, Manager, General Services Department
E. A. Womack, Manager, Plant Design

The inspector summarized the scope and findings of the inspection. Management comments were generally for clarification only, or acknowledgement of the statements by the inspector.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION IV
611 RYAN PLAZA DRIVE, SUITE 1000
ARLINGTON, TEXAS 76011

27 SEP 1978

THIS DOCUMENT HAS NOT BEEN
REVIEWED FOR PROPRIETARY
INFORMATION AS DESCRIBED
IN 10 CFR 2.790

Sheron
aB WR

Docket No. 99900403/78-03

The General Electric Company
Nuclear Energy Business Group
ATTN: Dr. R. H. Beaton
Vice President and Group Executive
175 Curtner Avenue
San Jose, California 95125

Gentlemen:

This refers to the QA Program inspection conducted by R. H. Brickley of this office on September 11-15, 1978, of your facility at San Jose, California and to the discussions of our findings with J. Barnard and members of your staff at the conclusion of the inspection.

Areas examined during the QA Program inspection and our findings are discussed in the enclosed report. Within these areas, the inspection consisted of an examination of procedures and representative records, interviews with personnel, and observations by the inspector.

During this inspection it was found that the implementation of your QA Program failed to meet certain commitments in your Topical Report No. NEDO-11209-04A. The specific findings and references to the pertinent requirements are identified in the enclosures to this letter.

Please provide us within thirty (30) days a written statement containing, (1) a description of steps that have been or will be taken to correct these items, (2) a description of steps that have been or will be taken to prevent recurrence, and (3) the dates your corrective actions and preventive measures were or will be completed.

In accordance with Section 2.790 of the Commission's "Rules of Practice," Part 2, Title 10, Code of Federal Regulations, a copy of this letter with enclosure and your reply together with the enclosed inspection report will be placed in the Commission's Public Document Room. If this report contains any information that you believe to be proprietary, it is necessary that you make a written application within thirty (30) days to this office to withhold such information from public disclosure. Any such application must include a full statement of the reasons on the basis of which it is claimed that the information is proprietary, and should be prepared so that proprietary information identified in the application is contained in a separate part of the document. If we do not hear from you in this regard within the specified period, the report will be placed in the Public Document Room.

Should you have any questions concerning this inspection, we will be pleased to discuss them with you.

Sincerely,

Uldis Potapovs

Uldis Potapovs, Chief
Vendor Inspection Branch

Enclosures:
1. Notice of Deviation
2. Inspection Report No. 99900403/78-03

bcc:
AD/RCI (REINMUTH)
IE FILES
NRR:DPM:QAB
REG. I, II, III, & V
PDR HQS
CENTRAL FILES
WEVETTER, RIV

The General Electric Company
Nuclear Energy Business Group
Docket No. 99900403/78-03

NOTICE OF DEVIATION

Based on the results of a NRC inspection conducted on September 11-15, 1978, it appeared that certain of your activities were not conducted in full compliance with NRC requirements as indicated below:

Criterion V (Instructions, Procedures, and Drawings) of Appendix B to 10 CFR Part 50 states in part, "Activities affecting quality shall be prescribed . . . and shall be accomplished in accordance with these instructions, procedures, or drawings." The corresponding Section 5 (Instructions, Procedures, and Drawings) of the General Electric Company Topical Report NEDO-11209-04A states in part, "Activities affecting quality, inculding methods of complying with 10 CFR 50, Appendix B, are delineated, accomplished, and controlled by such documents as policies, procedures, operating instructions, design specifications . . . ."

Contrary to the above, certain activities were not accomplished in accordance with your procedures as follows:

1. Subsection 4.2.d. of EOP 40-6.00 (Independent Design Verification) issued July 7, 1977, states in part, concerning the verifier, "Prepare a verification statement that the design document is verified . . . ." Additionally, Subsection 4.2.c. of EOP 40-10.00 (Design Record Files) states in part, "Develop DRF contents to provide documented traceable and retrievable evidence of technical activities undertaken, such as . . . Evidence of appropriate design verification."

   Contrary to the above, neither the verification statement nor other evidence of appropriate design verification was in the Design Record File for CHAST 06. Additionally, the file did not contain the results of a design review on September 23, 1977, of the gamma smearing model. It does appear; however, that the design verification was accomplished.

2. Exhibit B (Design Review Report) of EP&P 5.39 (Design Reviews) issued September 22, 1975, presents instructions for completion of the Design Review Report (DRR) for i.e., Type of Review (Conceptual, Preliminary, Problem, Final or Verification) and Discussion of Design Review Presentation (detailed text of design review proceedings).

   Contrary to the above, the DRR for the September 1, 1976, review of CHAST 05, Swelling and Rupture Model, did not indicate the Type of Review nor provide a Discussion of the Design Review Presentation.

3. Exhibit C (Design Review/Verification Cover Sheet) of EP&P 5.39 (Design Reviews) issued September 22, 1975, requires a statement of design adequacy per paragraph 5.2 which states, ". . . the review team shall in the reporting documentation establish a position which will provide either: a. An unconditional statement of design adequacy or b. A statement of adequacy conditional upon the resolution of certain specific documented open items . . . ."

   Contrary to the above, the Design Review/Cover Sheet for the CHAST 05 Swelling and Rupture Model, Design Review of September 1, 1976, did not have a statement of design adequacy.

VENDOR INSPECTION REPORT

U. S. NUCLEAR REGULATORY COMMISSION
OFFICE OF INSPECTION AND ENFORCEMENT
REGION IV

Report No. 99900403/78-03 Program No. 44082

Company: The General Electric Company
Nuclear Energy Business Group
175 Curtner Avenue
San Jose, California 95125

Inspection Conducted: September 11-15, 1978

Inspectors: R. H. Brickley 9/22/78
R. H. Brickley, Principal Inspector, Vendor Inspection Branch — Date

Donald G. Anderson 9/22/78
D. G. Anderson, Principal Inspector, Vendor Inspection Branch — Date

Other Personnel: R. H. Brickley 9/22/78
for J. Guttman, Nuclear Engineer, AB/NRR — Date

R. H. Brickley 9/22/78
for Z. R. Rosztoczy, Chief, AB/NRR — Date

R. H. Brickley 9/22/78
for B. W. Sheron, Nuclear Engineer, AB/NRR — Date

Approved by: C. J. Hale 9-26-78
C. J. Hale, Chief, Projects Section, Vendor Inspection Branch — Date

Summary

Special Inspection conducted on September 11-15, 1978 (99900403/78-03)

Areas inspected: 10 CFR 50, Appendix B, and Topical Report NEDO-11209-04A as applied to the establishment and implementation of procedures to control the development and revision of safety analysis computer codes. The inspection involved sixty-six (66) inspector hours on site by two (2) NRC, Region IV inspectors.

Results: In the area inspected there were no unresolved items and one deviation identified as follows:

Deviation: 10 CFR 50, Appendix B, Criterion V, and Section 5 of Topical Report NEDO-11209-04A - three (3) examples of a failure to follow procedures in the development and revision of safety analysis computer codes. (See Notice of Deviation, Enclosure.)

DETAILS SECTION

(Prepared by D. G. Anderson and R. H. Brickley)

A. Persons Contacted

L. S. Bohl, Manager, Design Review; Reliability Engineering; Nuclear Energy Engineering Division (NEED)
*J. D. Duncan, Manager, ECCS Engineering
*D. E. Lee, Manager, Quality Control; NEED
*R. B. Linford, Manager, Systems Dynamic Methods; NEED
*J. L. Murray, Manager, Quality Assurance; NEED
A. S. Rao, Technical Leader, ECCS Analysis; NEED
R. W. Schrum, Engineer, Systems Dynamic Methods
*B. S. Shiralkar, Manager, Thermal Hydraulic Methods; NEED
*J. M. Sorensen, Technical Leader, Thermal Hydraulic Methods; NEED
*J. E. Wood, Manager, Nuclear Core Technology; NEED
A. I. Yang, Responsible (REFLOOD)

*Denotes those present at the exit interview.

B. Introduction

This report covers a special inspection conducted to examine the establishment and implementation of procedures controlling safety analysis computer code development. The objectives of this inspection are:

1. To determine that adequate procedures to minimize the potential for analysis errors to go undetected have been established for control of the development and revision of these codes.

2. To determine that these procedures were fully implemented during the development and revision of selected codes.

C. Control of Safety Analysis Computer Codes

1. Establishment of Procedures

a. Inspection

(1) An examination of the NEED Engineering Operating Procedure (EOP) Manual, which contains procedures implementing Topical Report NEDO-11209-04A (Nuclear Energy Business Group Boiling Water Reactor Quality Assurance Program Description) revealed that procedure EOP 40-3.00

(Computer Programs) is the principal document governing this activity. Requirements for independent design verification, the design review program, and the design record files were found in EOPs 42-6.00, 40-7.00, and 42-10.00 respectively.

(2) The examination of EOP 40-3.00 (formerly EP&P 5.36) revealed that it defines responsibilities and procedural requirements for the control of digital and hybrid Engineering Computer Programs (ECP). The procedure was found to assign status levels for all ECPs that were defined as follows:

Level 1: ECPs under development and those not authorized for design applications.

Level 2: Approved Production Programs i.e., ECPs verified and documented for design applications and for all technical activities used in developing design related information.

Level 2R: Restricted Approved Production Programs i.e., ECPs that do not satisfy all requirements for Level 2, but may be applied to specfic design tasks with the approval of cognizant managment.

Level 3: Archive Programs i.e., ECPs approved for design use but which are no longer the most recent approved version.

Level 4: Historical Program i.e., ECPs that are inactive and not currently used for design.

This procedure further requires that:

An Encoded Technology Review be conducted in accordance with EOP 42-6.00 (Independent Design Verification), to provide independent verification and qualification of the ECP and Program Data Library before approval of a Level 2 status.

A Methods Procedures Committee be established to provide user/developer interfaces, technical specifications reviews, and appropriate assistance to control develment and use of ECPs.

Changes to ECPs be controlled via change verification and documentation, and reassignment of status levels.

An ECP Design Record File (DRF) be established and maintained in accordance with EOP 42-10.00 (Design Record Files).

(3) An examination of EOP 42-6.00 (formerly EP&P 5.38) revealed that the following four (4) methods of design verification were established: checking, alternate calculations, testing, or design review. When verification is by design review, the procedure requires the reviewers consider specified criteria i.e., the basic questions from subsection 6.3.1 of ANSI N45.2.11 plus additional NEED criteria. In addition, this procedure establishes factors which effect the extent of design verification, provides criteria on the verification method to be used, and assigns responsibility for the conduct of procedural activities.

(4) The examination of EOP 40-7.00 (formerly EP&P 5.39) revealed that reviews conducted under this program evaluate the adequacy of product designs including concepts, the design process, methods, analytical models, criteria, materials application, and development programs. These reviews may be used to verify that product designs meet functional, contract, safety, regulatory, industry code and standard, and GE requirements. This procedure also requires:

The establishment of a Design Review Board consisting of individuals independent of the item being reviewed.

The development of an Action Plan in response to design review open items which must identify specific action items, scheduled close-out, and the responsible individual.

The placement in the DRF of the Design Review Report, Action Plan, and action item completion when the design review is a part of design verification.

The written notification to Quality Assurance when significant design deficiencies appear to result from the engineering management system.

(5) The examination of EOP 42-10.00 (formerly EP&P 5.1.10) revealed that it requires the establishment of a DRF consisting of information related to a specific design

activity or engineering problem so as to provide traceable and retrievable documentation for design verification and satisfy GE, code, and regulatory design record requirements. The types of information to be placed in a DRF are listed e.g., design basis data, design notes, calculations, records, design conclusions, and evidence of appropriate design verification.

b. Findings

During the examination of the NEED procedures, the following items were identified and General Electric management stated they would consider further action, as appropriate. Any action taken by General Electric will be examined during a future inspection.

(1) EOP 40-3.00 (Computer Programs)

(a) The procedure does not provide a specific definition of originator, verifier, or reviewer e.g., neither the Methods Review Committee nor the Design Review Team are specified as the verifiers of the computer program.

(b) The procedure does not define what constitutes a qualified program.

(c) The procedure does not require a check of the formulation of the equations that make up the computer program.

(d) The procedure does not require that the Methods Committee document their review and concurrance with any restrictions on use of the computer program.

(e) The procedure does not require that a computer program known to have errors be retired.

(f) The procedure does not require that a warning notification be transmitted to the user organizations of record of a computer program found to contain an error.

(g) The procedure does not require a formal distribution of computer certification changes.

(h) The procedure does not impose a restriction on the length of time permitted to remove a computer program from the program Library following a Level 4 certification.

(i) The procedure does not require the signature of authorized personnel on computer program abstracts.

(j) The procedure does not require documentation of <u>all</u> computer program errors that are identified and the results of their evaluation.

(2) <u>EOP 42-6.00 (Independent Design Verification)</u>

(a) The procedure does not require the formal documentation of the contents of the Design Review Package and its submittal to each of the reviewers (Methods Review Committee/Design Review Team) prior to the review meeting.

(b) The procedure does not require the signature of authorized personnel on documentation of completion of responsibilities e.g., designate verifier, define extent, and depth of verification.

(c) The procedure does not require the verifiers of a computer program (Methods Review Committee/Design Review Team) to check the adequacy of the calculations used in the program check.

(3) <u>EOP 40.700 (Design Review Program)</u>

Although the DRT chairman must concur with the action plan, the procedure does not require that the Methods Review Committee/Design Review Team document the close-out and their acceptance of actions taken on open items and recommendations resulting from their review.

(4) <u>EOP 42-10.00 (Design Record Files)</u>

The procedure does not require that the Design Record File for a computer program contain a cross reference to other Design Record Files that contain documentation of activities performed as part of the review process e.g., a reference to the DRF containing verification calculations.

2. Implementation of Procedures

a. Inspection

The development and revision of computer programs CHASTE (Core Heatup Analyses Model) and REFLOOD(Analytical Model for Loss of Coolant Analysis) were selected by AB/NRR personnel for examination. The inspectors examined the DRFs maintained on these programs consisting of seven (7) topical reports, four (4) user manuals, seven (7) notices of design reviews, eighteen (18) design review reports, forty (40) IOMs, eight (8) design verification cover sheets, four (4) design review report/open items lists, seven (7) ECP status sheets, three (3) ECP abstracts, two (2) program logs, three (3) microfiche files, four (4) functional specifications, one (1) programmer's manual, three (3) computer program submittal forms, and one (1) design procedure.

b. Findings

(1) The IOMs examined covered a variety of subjects concerning these programs e.g., CHAST 06, Sensitivity Studies, dated July 13, 1977; Closure of CHAST 06 Design Review Open Items, dated October 25, 1977; Fuel Properties for LOCA Analysis dated February 5, 1978; GEGAP III - CHASTE Interface dated April 24, 1974; Minutes, Design Review Board, dated January 9, 1975; Response to Design Review Report - BWR LOCA Models, dated February 28, 1974; Design Review Board Minutes, BWR LOCA Evaluation Models, and Improvement Programs, dated July 11, 1975; Thermal Hydraulics and Transient Analysis Methods Procedures Committee Meeting Minutes, dated July 21, 1977; etc.

(2) Three (3) examples of a single deviation were identified. (See Notice of Deviation.)

(3) There were no unresolved items identified.

D. Exit Interview

An exit interview was held with management representatives on September 15, 1978. In addition to those individuals indicated by an asterick in paragraph A, those in attendance were:

J. Barnard, Manager, Nuclear Energy Product and Quality Assurance Operations (NEP&QAO)
R. C. Boesser, Manager, Quality Assurance and Operating Methods; Nuclear Energy Projects Division (NEPD)

A. Breed, Manager, Quality Assurance, NEP&QAO
D. L. Fischer, Manager, Nuclear Engineering, NEED
L. K. Holland, Manager, Plant Performance Engineering, NEED
A. I. Kaznoff, Manager, Product Assurance, NEP&QAO
A. J. Levine, Manager, Project Licensing #1, NEPD
D. F. Long, Manager, Engineering Services Operation, NEED
F. M. Paradiso, ECCS Engineering, NEED
W. J. Roths, Manager, Reliability Engineering Operation, NEED
H. E. Stone, Vice President and General Manager, NEED
R. N. Woldstad, Principal Licensing Engineer, NEPD

The inspector summarized the scope and findings of the inspection. Management comments were generally for clarification only, or acknowledgment of the statements by the inspector.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION IV
611 RYAN PLAZA DRIVE, SUITE 1000
ARLINGTON, TEXAS 76011

11 OCT 1978

THIS DOCUMENT HAS NOT BEEN REVIEWED FOR PROPRIETARY INFORMATION AS DESCRIBED IN 10 CFR 2.790
Sheron
DSS/RRR

Docket No. 99900404/78-03

Westinghouse Electric Corporation
ATTN: Dr. W. H. Arnold, General Manager
PWR Systems Division
Post Office Box 355
Pittsburgh, Pennsylvania 15230

Gentlemen:

This refers to the QA Program Inspection conducted by Mr. D. G. Anderson of this office on September 25-28, 1978, of your facility at Monroeville, Pennsylvania, and to the discussions of our findings with Mr. E. J. Kreh, and members of your staff at the conclusion of the inspection.

Areas examined during the QA Program inspection and our findings are discussed in the enclosed report. Within these areas, the inspection consisted of an examination of procedures and representative records, interviews with personnel, and observations by the inspector.

During this inspection it was found that the implementation of your Quality Assurance Program failed to meet certain NRC requirements. The specific findings and references to the pertinent requirements are identified in the enclosures to this letter.

Please provide us within thirty (30) days a written statement containing, (1) a description of any steps that have been or will be taken to correct this item, (2) a description of any steps that have been or will be taken to prevent recurrence, and (3) the dates your corrective actions and preventive measures were or will be completed.

In accordance with Section 2.790 of the Commission's "Rules of Practice," Part 2, Title 10, Code of Federal Regulations, a copy of this letter and your reply together with the enclosed inspection report will be placed in the Commission's Public Document Room. If this report contains any information that you believe to be proprietary, it is necessary that you make a written application within thirty (30) days to this office to withhold such information from public disclosure. Any such application must include a full statement of the reasons on the basis of which it is claimed that the information is proprietary, and should be prepared so that proprietary information identified in the application is contained in a separate part of the document. If we do not hear from you in this regard within the specified period, the report will be placed in the Public Document Room.

Westinghouse Electric
Corporation

-2-

Should you have any questions concerning this inspection, we will be pleased to discuss them with you.

Sincerely,

Uldis Potapovs, Chief
Vendor Inspection Branch

Attachment:
1. Notice of Deviation
2. Inspection Report No. 99900404/78-03

bcc:
AD/RCI (REINMUTH)
IE FILES
NRR:DPM:QAB
REG. I, II, III, & V
PDR HQS
CENTRAL FILES
WEVETTER, RIV

VENDOR INSPECTION REPORT

U. S. NUCLEAR REGULATORY COMMISSION
OFFICE OF INSPECTION AND ENFORCEMENT
REGION IV

Report No. 99900404/78-03 Program No. 44081

Company: Westinghouse Electric Corporation
Pressurized Water Reactor Systems Division
P. O. Box 355
Pittsburgh, Pennsylvania 15230

Inspection Conducted: September 25-28, 1978

Inspectors: Donald G. Anderson 10/5/78
D. G. Anderson, Principal Inspector, Vendor Inspection Branch — Date

R. H. Brickley 10/5/78
R. H. Brickley, Principal Inspector, Vendor Inspection Branch — Date

Other Personnel: Donald G. Anderson 10/5/78
for/ B. W. Sheron, Nuclear Engineer, DSS/NRR — Date

Donald G. Anderson 10/5/78
for/ G. N. Lauben, Nuclear Engineer, DSS/NRR — Date

Donald G. Anderson 10/5/78
for/ M. W. Hodges, Principal Reactor Engineer DSS/NRR — Date

Approved by: R. H. Brickley 10/5/78
for C. J. Hale, Chief, Projects Section, Vendor Vendor Inspection Branch — Date

Westinghouse Electric Corporation
Docket No. 99900404/78-03

NOTICE OF DEVIATION

Based on the results of an NRC inspection conducted on September 25-28, 1978, it appeared that certain of your activities were not conducted in full compliance with NRC requirements as indicated below:

Criterion V (Instructions, Procedures, and Drawings) of Appendix B to 10 CFR Part 50 states in part, "Activities affecting quality shall be prescribed . . . and shall be accomplished in accordance with these instructions, procedures, or drawings." The corresponding applicable Section, 17.1.5 (Instructions, Procedures, and Drawings) of the Westinghouse Topical Report, WCAP 8370, states in part, "The Quality Assurance Program provides that activities affecting quality will be accomplished in accordance with documented instructions, procedures and drawings . . . ."

Contrary to the above, procedures do not exist describing the method by which changes to the evaluation model are reported in amendments submitted to the NRC as required by paragraph 1.b. of Section II of 10CFR50, Appendix K. (See Section D. 2.b.)

Summary

Special Inspection conducted on September 25-28, 1978 (99900404/78-03)

Areas Inspected: 10 CFR 50, Appendix B, and Topical Report WCAP 8370 as applied to the establishment and implementation of procedures to control the development and revision of safety analysis computer codes. The inspection involved fifty-six (56) inspector hours on site by two (2) USNRC Region IV inspectors.

Results: In the area inspected there were no unresolved items and one (1) deviation identified as follows:

Deviation: 10 CFR 50, Appendix B, Criterion V, and Section 17.1.5 of Topical Report WCAP 8370-procedures do not exist for the evaluation and reporting of significant changes in the evaluation model as referenced in Criterion II.b. of 10 CFR 50, Appendix K. (See Notice of Deviation, Enclosure.)

DETAILS SECTION

(Prepared by D. G. Anderson and R. H. Brickley)

A. Persons Contacted

*L. A. Campbell, Senior Engineer
*R. A. Dannels, Manager, Methods Development
*V. J. Esposito, Manager, Safeguards Engineering
S. M. Hendley, Advisory Scientist
*R. A. Margolis, Senior Engineer
*J. J. McInerney, Senior Quality Assurance Engineer
P. T. McManus, Senior Quality Assurance Engineer
*R. A. Muench, Manager, Safeguards Analysis
*R. W. Steitler, Manager, Reactor Protection Analysis

*Denotes those present at the exit meeting.

B. Action on Previous Inspection Findings

1. (Open) Deviation (Report No. 77-02): Records which were not yet in the permanent storage facility were not being maintained in duplicate sets in separate geographical locations. Corrective action on this item is still in progress. Westinghouse has commited to the completion of filming, jacketing, and transfer of all equipment descriptions, system descriptions, and QA specifications to the Boyers Records Center by the end of December, 1978. This item will be inspected when corrective action is completed.

2. (Closed) Deviation (Report No. 78-02): Several computer program abstract forms (55374) had not been approved by the immediate manager. The inspector reviewed the corrective actions described in the Westinghouse letter of response dated September 15, 1978, and confirmed that the computer program abstract forms identified in the inspection report had been signed by the immediate manager. The inspector also reviewed a memorandum dated August 18, 1978, which instructed all personnel in Configuration Control (Methods Development) to only accept forms which has been completed as required.

C. Introduction

This report covers a special inspection conducted to examine the establishment and implementation of procedures controlling safety analysis computer code development. The objectives of this inspection are:

1. To determine that adequate procedures to minimize the potential for analysis errors to go undetected have been established for control of the development and revision of these codes.

2. To determine that these procedures were fully implemented during the development and revision of selected codes.

D. Control of Safety Analysis Computer Codes

1. Establishment of Procedures

a. Inspection

(1) The Westinghouse-PWRSD Topical Report, WCAP 8370, requires in Section 17.1.3, Design Control that "Where computer programs are used in design analysis, these programs are verified and their usage is controlled." These commitments are implemented by the following Westinghouse Electric Corporation-Nuclear Energy Systems-Water Reactor Divisions Policy and Procedures:

(a) OPR-ND-300-1, Verification and Qualification of Computer Programs Used in Engineering Analysis, Design, or Safety Analysis (Policy).

(b) OPR-300-5, Configuration Control of Computer Programs (Procedure).

(2) An examination of OPR-300-1 revealed that there are requirements for verification of computer programs and documentation of that verification for inclusion in a Central Program File Package which is then maintained by the Configuration Control Section of Methods Development. Appendix A of this Policy outlines nine (9) alternatives for verification of a computer program and ten (10) alternatives for qualification of a computer program.

(3) An examination of OPR-300-5 revealed that requirements for the submission of new computer programs and the modification of existing computer programs are established along with the definition of responsibilities of individuals in the verification chain. The computer program forms which make up a portion of the verification documentation are included as Appendix C.

(4) The Nuclear Safety Procedures Manual contains the implementing procedures to be used at the departmental

level. Since this special inspection was restricted to computer codes used in safety analyses, the applicable group procedures within the Nuclear Safety Department were as follows:

(a) General; Procedure 1.1, Configuration Control of Computer Programs.

(b) Reactor Protection; Procedure 4.5, Preparation of SAR Analyses; Procedure 4.6, Preparation and Review of Calculation Notes; Procedure 4.12, Qualification of Computer Codes Used by Reactor Protection.

(c) Methods Development: Procedure 6.2.1, Quality Assurance of Reactor Code Systems (QUARCS) Benchmark Library; Procedure 6.2.2, Quality Assurance of Reactor Code Systems (QUARCS) Testing Programs with Benchmarks; Procedure 6.3, Preparation/Preservation of Verification Documentation.

(d) Safeguards Engineering: Procedure 5.2, Preparation of Design Analyses; Procedure 5.3, Preparation of Calculation Notes; Procedure 5.4, Generation of Safeguards Engineering Standards.

b. <u>Findings</u>

The procedures used to implement WCAP 8370 appear to meet the requirements of ANSI N45.2.11 as appropriate to verification, and documentation of this verification for safety analysis computer codes. During the examination of these implementing procedures, the following items were identified and Westinghouse management indicated that they would consider further action, as appropriate. Any action taken by Westinghouse will be examined during a future inspection.

(1) Procedures do not address how errors identified in computer programs are reported to the USNRC.

(2) Procedures do not address how warning statements regarding restrictions on code use are resolved.

(3) Microfische records used in engineering analysis are not always legible.

(4) Documentation did not specify which codes constituted the LOCA/ECCS evaluation model.

(5) The meaning of independent verification is not clearly identified on the Computer Program Change Request Form (55375).

(6) Procedures do not require the reexamination and reevaluation of procedures in the event of code errors.

(7) Ancillary codes referred to in computer program documents are not described or referenced adequately.

(8) Procedures do not address the correction of errors identified in computer program WCAP documents.

(9) Safety Analysis Standards do not sufficiently identify code input options.

(10) Procedures do not address comparison of new versions of codes against the same data used to verify the original version.

(11) Standard No. 19 of the Safety Analysis Standard references an out-of-date version of a computer code.

(12) Procedures do not address updating of Safety Analysis Standards.

2. Implementation of Procedures

a. Inspection

The development and revision of the following computer programs was evaluated for meeting the requirements of OPR-300-1 and OPR-300-5 related to verification and control:

LOCTA IV: A computer code designed to calculate the wall temperatures of the fuel rod, average pellet temperature, average clad temperature, and fluid temperatures during the loss of coolant accident (LOCA).

LOFTRAN: A digital computer code which calculates the detailed transient behavior of a one loop pressurized water reactor system.

The inspectors examined the documentation contained in the Central Program File Package on these two (2) computer programs which consisted of five (5) memoranda transmitted between Westinghouse and the USNRC, twelve (12) internal memoranda transmitted between departments in Westinghouse, twelve (12) computer code topical reports contained in WCAP documents, twenty-nine (29) calculation notes, one (1) Safety Review Committee meeting minutes, four (4) Computer Configuration Control Forms, twenty-two (22) Computer Code Change Request forms, three (3) Safeguards Engineering Standards, one (1) copy of the Safety Analysis Standards, nineteen (19) computer program runs on microfilm, and three (3) Chronological Code Change Index forms.

b. Findings

In this area of the inspection, no unresolved items were identified. One (1) deviation from commitment was identified (See Notice of Deviation, Enclosure).

Additional information related to this deviation was noted during the review of calculation notes for the zirconium-water reaction error analysis. These calculation notes reported that after modifications had been made to LOCTA IV, recalculated values for the peak clad temperature resulted in a temperature increase of 24°F. It was further noted that no followup action on this item had been performed nor were model changes identified in the resubmitted topical report (WCAP 9220). With respect to this item, paragraph 1.b. of Section II of 10CFR50, Appendix K, requires that "The description (of the evaluation model) shall be sufficiently detailed and specific to require significant changes in the evaluation model to be specified in amendments of the description. For this purpose, a significant change is a change that would result in a calculated fuel cladding temperature different by more that 20°F from the temperature calculated (as a function of time) for a postulated LOCA using the last previously accepted model." DSS/NRR will followup on this item to determine if reporting requirements have been met by Westinghouse.

E. Exit Meeting

An exit meeting was conducted with management representatives at the conclusion of the inspection on September 28, 1978. In addition to those individuals indicated by an asterisk in Section A. of the Details Section of this report, the following were in attendance:

T. M. Anderson, Manager, Nuclear Safety
J. A. Burgess, Manager, Quality Assurance
E. S. Hampton, Manager, Product Assurance Programs
G. G. Harkness, Systems Analyst

K. R. Jordan, Manager, Reactor Protection
E. J. Kreh, Manager, Product Assurance
D. C. Richardson, Manager, Reactor Protection Analysis
R. A. Wiesemann, Manager, Regulatory and Legislative Affairs

The inspector summarized the outstanding items and the corrective action which was reviewed during this inspection. The inspector discussed the scope and findings identified during this inspection. Management representatives acknowledged the statements by the inspector with respect to the one (1) deviation presented.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
REGION IV
611 RYAN PLAZA DRIVE, SUITE 1000
ARLINGTON, TEXAS 76011

27 NOV 1978

THIS DOCUMENT HAS NOT BEEN
REVIEWED FOR PROPRIETARY
INFORMATION AS DESCRIBED
IN 10 CFR 2.790
B. Sheron
DSS/NRR

Docket No. 99900401/78-04

Combustion Engineering, Inc.
Attn: Mr. M. R. Etheridge
Vice President
General Services
1000 Prospect Hill Road
Windsor, Connecticut 06095

Gentlemen:

This refers to the QA Program Inspection conducted by Mr. D. G. Anderson of this office on November 13-17, 1978, of your facility at Windsor, Connecticut, and to the discussions of our findings with Mr. C. W. Hoffman and members of your staff at the conclusion of the inspection.

Areas examined during the QA Program inspection and our findings are discussed in the enclosed report. Within these areas, the inspection consisted of an examination of procedures and representative records, interviews with personnel, and observations by the inspector.

During this inspection it was found that the implementation of your Quality Assurance Program failed to meet certain NRC requirements. The specific findings and references to the pertinent requirements are identified in the enclosures to this letter.

Please provide us within thirty (30) days a written statement containing, (1) a description of any steps that have been or will be taken to correct this item, (2) a description of any steps that have been or will be taken to prevent recurrence, and (3) the dates your corrective actions and preventive measures were or will be completed.

In accordance with Section 2.790 of the Commission's "Rules of Practice," Part 2, Title 10, Code of Federal Regulations, a copy of this letter and your reply together with the enclosed inspection report will be placed in the Commission's Public Document Room. If this report contains any information that you believe to be proprietary, it is necessary that you make a written application within thirty (30) days to this office to withhold such information from public disclosure. Any such application must include a full statement of the reasons on the basis of which it is claimed that the information is proprietary, and should be prepared so that proprietary information identified in the application is contained in a separate part of the document. If we do not hear from you in this regard within the specified period, the report will be placed in the Public Document Room.

Should you have any questions concerning this inspection, we will be pleased to discuss them with you.

Sincerely,

Uldis Potapovs, Chief
Vendor Inspection Branch

Enclosures:
1. Notice of Deviation
2. Inspection Report No. 99900401/78-04

bcc:
AD/RCI (REINMUTH)
IE FILES
NRR:DPM:QAB
REG. I, II, III, & V
PDR HQS
CENTRAL FILES
HEVETTER, RIV

Combustion Engineering, Inc.
Docket No. 99900401/78-04

NOTICE OF DEVIATION

Based on the results of an NRC inspection conducted on November 13-17, 1978, it appeared that certain of your activities were not conducted in full compliance with NRC requirements as indicated below:

Criterion V (Instructions, Procedures, and Drawings) of Appendix B to 10 CFR Part 50 states in part, "Activities affecting quality shall be prescribed . . . and shall be accomplished in accordance with these instructions, procedures, or drawings."

Contrary to the above, procedures do not exist describing the method by which changes to the evaluation model are reported in amendments submitted to the NRC as required by paragraph 1.b. of Section II of 10 CFR 50, Appendix K.

U. S. NUCLEAR REGULATORY COMMISSION
OFFICE OF INSPECTION AND ENFORCEMENT
REGION IV

Report No. 99900401/78-04 Program No. 51100

Company. Combustion Engineering, Inc.
1000 Prospect Hill Road
Windsor, Connecticut 06095

Inspection Conducted: November 13-17, 1978

Inspectors: 11-28-78
D. G. Anderson, Principal Inspector, Date
Vendor Inspection Branch

Other Personnel: 11-28-78
B. W. Sheron, Nuclear Engineer, OSS/NRR Date

11-28-78
G. N. Lauben, Nuclear Engineer, OSS/NRR Date

11-28-78
P. E. Norian, Section Leader, OSS/NRR Date

Approved by: 11-29-78
C. J. Hale, Chief, Vendor ~~Program~~ Evaluation Section, Vendor Inspection Branch Date

Summary

Special Inspection conducted on November 13-17, 1978 (99900401/78-04)

Areas Inspected: 10 CFR 50, Appendix B, and Topical Report CENPD-210-A as applied to the establishment and implementation of procedures to control

the development and revision of safety analysis computer codes. The inspection involved thirty (30) inspector hours on site by one (1) USNRC Region IV inspector.

Results: In the area inspected one deviation and one unresolved item were identified as follows:

Deviation: 10 CFR 50, Appendix B, Criterion V, procedures do not exist for the evaluation and reporting of significant changes in the evaluation model as referenced in Criterion II.b. of 10 CFR 50, Appendix K. (See Notice of Deviation, Enclosure.)

Unresolved Item: Verification had not been completed on two (2) calculations which resulted in input to the CESSAR System 80 FSAR (See Details Section paragraph C.2.b.).

DETAILS SECTION

(Prepared by D. J. Anderson)

A. Persons Contacted

*W. C. Coppersmith, Manager, Design Transients Safety Analysis
F. L. Carpentino, Section Manager, ECCS Analysis Group
*J. Goldberg, Supervisor, Standard Plant Licensing
*F. G. Harvey, Engineering Quality Assurance Auditor
*C. L. Kling, Acting Supervisor, CESEC Development Group
J. Longo, Jr., Manager, ECCS Analysis Group
H. T. Melcher, Engineering Specialist
*R. R. Mills, Supervisor, Project and Generic Licensing
*J. C. Packard, Supervisor, Group Quality Systems

*Denotes those present at the exit meeting.

B. Introduction

This report covers a special inspection conducted to examine the establishment and implementation of procedures controlling safety analysis computer code development. The objectives of this inspection were:

1. To determine that adequate procedures to minimize the potential for analysis errors to go undetected have been established for control of the development and revision of these codes.

2. To determine that these procedures were fully implemented during the development and revision of selected codes.

C. Control of Safety Analysis Computer Codes

1. Establishment of Procedures

a. Inspection

(1) The Combustion Engineering, Inc., Topical Report CENPD-210-A, requires in Section 17.3, Design Control, that "The QADM procedures implement design quality assurance requirements . . . provide specific requirements for all safety related work accomplished . . . provide design controls to applicable activities such as; reactor physics, seismic, stress, thermal, hydraulic, radiation and accident analysis . . . contains an identification system for analyses and/or calculations

prepared for each NSSS project within the section. This indicates how calculation sheets will be completed. Methods of analyses in the form of computer programs are controlled by the procedure. The computer programs that are used for safety-related analyses are certified for accuracy, method, and internal consistency prior to verification of the analysis in which it is used."

These commitments are implemented by the following Combustion Engineering, Inc., procedures:

QADP 5.2, Design Analysis
QADP 5.4, Design Verification

(2) An examination of procedure QADP 5.2 revealed that there are detailed requirements for the preparation, review, and verification of analyses and computer codes. Requirements for documentation of this verification are also included in the procedure. Changes to analyses or computer programs shall comply with the requirements for initial preparation of the analyses or computer programs. A Computer Code Certificate is the permanent file identification for computer codes that have been certified by Combustion Engineering, Inc.

(3) An examination of procedure QADP 5.4 revealed that Combustion Engineering, Inc., utilizes three distinct methods of design verification: Design Reviews, Alternate Calculations/Analyses, and Testing. A list of qualified reviewers is maintained by each Supervisor/Manager and independent review of analyses/calculations is conducted by reviewers selected from this list.

b. <u>Findings</u>

QADP 5.2 and QADP 5.4, which are procedures used to implement CENPD-210-A, appear to meet the requirements of ANSI N45.2.11 as appropriate to verification, and documentation of this verification, as applied to Safety Analysis Computer Codes. During the examination of these implementing procedures and the documentation generated as a result of following the procedures, the following items were identified and management of Combustion Engineering, Inc., indicated that they would consider further action, as appropriate. Any action taken by Combustion Engineering, Inc., will be examined during a future inspection.

In addition to the items listed below, one (1) deviation from commitment was identified (See Notice of Deviation, Enclosure). No unresolved items were identified in this area of the inspection.

Items for consideration by Combustion Engineering, Inc., Management:

(1) There does not appear to be any central index to define what constitutes the code design file, or a project design file.

(2) Procedures do not address how modifications to NRC-approved codes are reported to NRC.

(3) The "ECCS Licensing Analysis Verification Checklist" was found in the system 80 CEFLASH calculation input file, but not in other files. We encourage the use of such a checklist for all calculations and its inclusion in the design files.

(4) There appears to be no information in the ECCS code files regarding verification by comparison to test data. Such comparisons are available through programs such as the standard problem program. We believe this form of verification to be applicable to parts of evaluation model codes and should be included in the code verification files.

(5) On the ECCS Licensing Analysis Verification Checklist, item 25 was checked "yes," indicating experimental data was employed. No evidence of how the experimental data was employed was found.

(6) Procedures do not address how errors identified in codes are dispositioned.

(7) A chronological listing of development, review, approval, and changes to codes had not been documented.

(8) Procedures do not address the process to be followed when existing codes are used in applications other than those for which the code was originally developed.

(9) Procedures do not address how documentation is maintained for the following items:

(a) Comparison of Codes with previous results.

(b) Review of Computer Code Quality Assurance Folders.

(c) Changes to Computer Codes.

(10) Departmental level procedures do not exist which address code development, review, approval, and control of computer codes.

(11) CESSAR/FSAR/System 80 LOCA Analyses were submitted to NRC prior to the completion of independent review of the analyses. QA review and verification of all documents should be completed prior to submittal to NRC.

(12) Procedures do not address how individual codes are to be used in an overall analysis model or package. Also, there are no requirements for assuring that integral results developed from more than one code are independently reviewed.

2. Implementation of Procedures

a. Inspection

The development and revision of the following computer programs was evaluated for meeting the requirements of QADP 5.2 and QADP 5.4 related to development, verification, and control of:

STRIKIN II: A Cylindrical Geometry Fuel Rod Heat Transfer Program. The STRIKIN II code is a Fortran IV digital program which is used to calculate the core hot spot transient clad temperature during the blowdown, refill, and reflood portions of the loss-of-coolant accident.

CESEC: Digital Simulation of a Combustion Engineering Nuclear Steam Supply System. Simulates doppler and moderator reactivity feedback, point kinetics neutron behavior, boron and CEA reactivity effects, multi-node average and hot channel reactor core thermal hydraulics, reactor coolant pressurization and mass transport, reactor coolant system safety valves, steam generation, steam generator water level, main steam bypass system, safety and turbine valves, as well as alarm, control, protection and Engineered Safety Feature Systems.

The inspector examined the documentation contained in the Quality Assurance Folder on these two (2) computer codes which consisted of fourteen (14) computer code Topical Reports, thirty-one (31) copies of interoffice correspondence twenty-four (24) calculations, seven (7) computer code certificates, ten (10) lists of qualified reviewers, six (6) analysis cover sheets, one (1) ECCS licensing analysis checklist, one (1) listing of the STRIKIN II code version 77036, and two (2) film cassettes of computer code verification runs.

b. Findings

In this area of the inspection, no deviations were identified. The following finding has been identified as an unresolved item and will be forwarded to NRC/NRR for resolution:

During a review of the verification of two (2) calculations that resulted in input to the CESSAR System 80 FSAR, sections 6.2.1.5 and 6.3.3., the inspector noted that the verification process had not been completed even though the FSAR has been submitted to NRR/NRC for docketing. Upon discussion of this item with Combustion Engineering representatives, it was noted that design input for these calculations had not as yet been received and therefore the calculations could not be completed and consequently could not be verified. 10 CFR 50.b.(4) requires that for Final Safety Analysis Reports that "A final analysis and evaluation of the design and performance of structures, systems and components with the objective stated in (a)(4)* of this section and taking into account any pertinent information developed since the submittal of the preliminary safety analysis report."

*(a)(4) refers to preparation of preliminary analyses.

The inference above to "final analysis" indicates that information should not be submitted to NRR/NRC which is "preliminary" in nature.

As noted before, this item will be forwarded to NRR/NRC for resolution of what constitutes "final analysis" for purposes of FSAR submittals.

D. Exit Meeting

An exit meeting was conducted with Combustion Engineering management personnel at the conclusion of the inspection. Those individuals indicated by an asterisk in Section A of the Details Section of this report were in attendance. In addition, the following were present:

J. M. Cicerchia, Licensing Engineer
E. P. Flynn, Director, Plant Apparatus and Engineering Quality Assurance
C. W. Hoffman, Director, Group Quality Assurance
G. J. Huba, Manager, Engineering Quality Assurance

The inspector discussed the special nature of this inspection, scope, and findings identified during the inspection. Management representatives of Combustion Engineering acknowledged the statements by the inspector with respect to the one (1) deviation presented.

Appendix C

Vendor Responses to IE

Inspection Reports

GENERAL ELECTRIC

NUCLEAR ENERGY BUSINESS GROUP

GENERAL ELECTRIC COMPANY, 175 CURTNER AVE., SAN JOSE, CALIFORNIA 95125

October 20, 1978

United States Nuclear Regulatory Commission
Office of Inspection and Enforcement, Region IV
611 Ryan Plaza Drive, Suite 1000
Arlington, Texas 76011

Attention: Mr. U. Potapovs, Chief
Vendor Inspection Branch

Reference: Inspection Report 99900403/78-03
Document No. 99900403/78-03
Program No. 44802

Gentlemen:

This is in response to your September 27, 1978, letter which contained the results of the QA Program Inspection of the Nuclear Energy Business Group's facility at San Jose, California, conducted by your office on September 11-15, 1978. Your letter was received in Dr. R. H. Beaton's office on October 2, 1978. Dr. Beaton has requested that I respond to your letter on his behalf.

We find nothing in this report of a proprietary nature which should be withheld from public disclosure.

The report identifies three areas in which there were deviations. The deviations with our responses are as follows:

1. Independent Design Verification

   Deviation
   Neither the verification statement nor other evidence of appropriate design verification was in the Design Record File for CHAST 06. Additionally, the file did not contain the results of a design review on September 23, 1977, of the gamma smearing model. It does appear, however, that the design verification was accomplished.

   Response
   A verification statement and other evidence of appropriate design verification, along with a copy of the Design Review Report (DRR), will be

properly filed in the Design Record File for the CHAST Engineering Computer Program.

2. Design Review Report/Design Reviews

Deviation
The DRR for the September 1, 1976, review of CHAST 05, Swelling and Rupture Model, did not indicate the Type of Review nor provide a Discussion of the Design Review Presentation.

Response
The Chairman of the design review team which performed the original review will prepare a statement to be attached to the Design Review Report. This statement will include the purpose, type of review, and briefly describe the type of information that was considered. The Design Review Report will then be filed in the CHAST Design Record File.

3. Verification Cover Sheet

Deviation
The Design Review/Cover Sheet for the CHAST 05 Swelling and Rupture Model, Design Review of September 1, 1976, did not have a statement of design adequacy.

Response
A statement containing the findings of the design review team and their conclusion as to the adequacy of the design will be prepared and signed by the Chairman of the design review team which performed the review in question. This statement will be attached to the original Design Review Report and will be properly filed in the CHAST Engineering Computer Program Design Record File.

The actions outlined above for correcting the deviation as cited by the noted three items will be completed by December 20, 1978.

In order to determine if these types of discrepancies exist in other computer programs, a formal evaluation program has been initiated. This evaluation will include those computer programs for licensing analyses in the ECCS and Transient areas and will be completed by January 15, 1979. If any similar examples of deviations are identified, an action plan for corrective action will be put in place and a schedule for completion will be specified by January 30, 1979.

To prevent any future occurrence of similar deviations, a training class will be initiated. Information is now being compiled which will form the basis of special training classes to be attended by methods committee members and responsible engineers of engineering computer programs used for licensing analysis in the ECCS and Transient areas. These training sessions will be specifically designed to instruct the individuals as to the required action to prevent future recurrences of the types of deviations identified by the NRC Audit. These training sessions will be completed by the end of the first quarter of 1979.

In addition to the above deviations, there were findings listed in paragraph C.1.b. on page 6 of the inspection report. Each of the findings identified in paragraph C.1.b. are being carefully evaluated by management. Following this evaluation, any appropriate action will be specified and scheduled. All required actions will be documented in order to satisfy the requirements of an issued Engineering Work Authorization which outlines the findings to be reviewed. The responses will contain either a description of any planned procedural changes, or the basis on which it is concluded by management that no procedural change is required. All of these actions will be completed by March 1, 1979.

I believe the foregoing information meets your request for responses to the inspection report. If further information is required, please let me know.

John Barnard

John Barnard

JB:AB:es

cc: Dr. R. H. Beaton
Mr. A. Breed

EXXON NUCLEAR COMPANY, Inc.

2101 Horn Rapids Road
P. O. Box 130, Richland, Washington 99352
Phone: (509) 943-8100 Telex: 32-6353

December 19, 1978

U. S. Nuclear Regulatory Commission
Region IV
611 Ryan Plaza Drive, Suite 1000
Arlington, Texas 76011

ATTENTION: Mr. Uldis Potapovs, Chief
Vendor Inspection Branch

Gentlemen:

Your letter dated November 22, 1978 reported findings regarding the audit conducted by Mr. D. G. Anderson of your organization on October 30 through November 3, 1978. Your letter stated it appeared that certain of ENC's activities were not conducted in full compliance with NRC requirements. These activities were as follows:

1. Procedures do not exist describing the method by which changes to the evaluation model are reported in amendments submitted to the NRC as required by Paragraph 1.b. of Section II of 10CFR50, Appendix K.

2. In two cases, calculation forms had not been completed and calculation indexes had not been prepared as required by Procedure XN-NF-S00,002, Section 6.0, Design Process.

In regard to these two items you requested that ENC provide "a written statement containing (1) a description of any steps that have been or will be taken to correct this item, (2) a description of any steps that have been or will be taken to prevent recurrence, and (3) the dates...corrective actions and preventive measures were or will be completed."

In response to Item (1), our procedure for reporting changes to an evaluation model will be included in XN-NF-S00,002. This change in our Quality Assurance procedure will formalize ENC's current practice for reporting code changes. Thus, this action neither corrects nor prevents recurrence of a safety consideration. We anticipate that the indicated change will be incorporated by March 1, 1979.

In regard to Item (2) above, ENC is continuing to follow XN-NF-S00,002, Section 6, with respect to the use of forms and calculational indexes. This includes appropriate personnel instruction and training. We believe the current practices in regard to this procedure assure a minimal number of procedural deviations and that those procedural deviations which may occur would continue to be of minor significance.

AN AFFILIATE OF EXXON CORPORATION

C-4

Your letter also listed "Findings" regarding other general observations relating to computer codes. These "Findings" principally addressed the implementation of additional formal procedures for computer code development, control, and use. Although ENC believes its present practices are effective in minimizing the possibility of errors, the advisability of changes to ENC procedures related to the "Findings" identified in your letter is being considered.

Sincerely,

Gerald Owsley

G. F. Owsley, Manager
Reload Licensing

GFO:gf

EXXON NUCLEAR COMPANY, Inc.

2101 Horn Rapids Road
P. O. Box 130, Richland, Washington 99352
Phone: (509) 943-8100 Telex: 32-6353

January 18, 1979

U. S. Nuclear Regulatory Commission
Region IV
611 Ryan Plaza Drive, Suite 1000
Arlington, Texas 76011

ATTENTION: Mr. Uldis Potapovs, Chief
Vendor Inspection Branch

Gentlemen:

In your letter dated December 29, 1978 you advised us that you needed additional information regarding Item 2 of your November 22, 1978 letter. Specifically, you asked that we provide the following information:

1. Your corrective action concerning the two specific cases identified where calculational forms (for calculations E-0157-2-33-P and E-0478-965-3) were not completed and prepared in accordance with your procedure; your further actions to assure that these were the only incorrect calculational forms; and the date these corrective actions were or will be completed.

2. Your specific preventative actions to assure this procedure will be followed in the future (e.g., retraining/indoctrination of user personnel and/or increased QA audit emphasis in this area) and the date those actions will be completed.

The first of the two specific cases which you referred to involved failure of the person checking input to a licensing calculation to sign that the input had been checked. Following your audit, the check was documented by his signature on the input listing. This deviation, which occurred in 1974 shortly after implementation of the applicable QA procedure, happened when individuals involved in carrying out this work were first becoming familiar with the applicable QA requirements. Subsequent training and indoctrination emphasized the procedural requirements for checking and signing input to final calculations, whether for design or licensing purposes.

The second case referred to involved failure to sign that the output of a safety analysis calculation had been appropriately reviewed and checked. However, as is ENC's standard practice, the results had been reviewed and checked as required by the analyst and a qualified second party against previous analyses. Following your audit, the check by the qualified second party was documented by his signature of the calculation output. ENC does not consider this deviation to be a failure to meet safety standards since the required action was taken. However, this incident was published within the organization to emphasize the necessity for appropriately signing and documenting that QA procedures have been followed for computer output information.

No further corrective action regarding these specific deviations is planned since these deviations did not involve failure to carry out appropriate safety-related action. However, compliance with verification requirements of the QA procedure will continue to be routinely checked during future Quality Assurance audits.

Sincerely,

G. F. Owsley, Manager
Reload Licensing

GFO:gf

Westinghouse Electric Corporation

Water Reactor Divisions

W H Arnold
General Manager
PWR Systems Division

Nuclear Center
Box 355
Pittsburgh Pennsylvania 15230

November 3, 1978

PAP-EJH-78-424

Mr. U. Potapovs, Chief
Vendor Inspection Branch
U. S. Nuclear Regulatory Commission
611 Ryan Plaza Drive
Suite 1000
Arlington, Texas 76011

Ref: a) Letter from USNRC (Mr. Pota:
to W (W. H. Arnold) dated
10/11/78

Subject: Response to September, 1978 Audit of Westinghouse PWRSD
(Docket No. 99900404/78-03)

Dear Mr. Potapovs:

Your letter (Ref. a) does not contain any information considered proprietary to Westinghouse and we have no objection to placement of the report in the Public Document Room. The response to the deviation resulting from the subject audit is as follows:

Deviation

"Based on the results of an NRC inspection conducted on September 25-28, 1978, it appeared that certain of your activities were not conducted in full compliance with NRC requirements as indicated below:

Criterion V (Instructions, Procedures, and Drawings) of Appendix B to 10 CFR Part 50 states in part, "Activities affecting quality shall be prescribed . . . and shall be accomplished in accordance with these instructions, procedures, or drawings." The corresponding applicable Section, 17.1.5 (Instructions, Procedur and Drawings) of the Westinghouse Topical Report, WCAP 8370, states in part, "Th Quality Assurance Program provides that activities affecting quality will be accomplished in accordance with documented instructions, procedures and drawings

Contrary to the above, procedures do not exist describing the method by which changes to the evaluation model are reported in amendments submitted to the NRC as required by paragraph 1.b. of Section II of 10CFR50, Appendix K. (See Sectio D.2.b. of Inspection Report 99900404/78-03 for additional details).

Response

OPR-600-1 and Nuclear Safety Procedure 1.9 cover reporting of any significant errors in any safety related work. Significant errors in computer codes have been and will continue to be reported under this procedure as with other significant errors discovered in the course of our work. Appendix K of 10CFR50 requires separate reporting of changes to NRC reviewed computer codes which result in a 20°F or more change in calculated peak clad temperature. Westinghouse has maintained a policy of identifying any such changes to the NRC.

Although these policies are well known and recognized by those performing safety related work, Nuclear Safety Procedure 5.2 will be modified to include the following statement in the "Policy and Scope" section:

> In addition, it is Safeguards Engineering Policy to evaluate and report significant changes in the evaluation model as referenced in Criterion II.B of 10CFR50 Appendix K. For significant errors, Procedure OPR-600-1 and NS Procedure 1.9 applies.

Further, the response to the items identified in paragraphs D.1.b. and D.2.b. of the subject report are also provided in the attachment. These were identified and agreed to at the Exit Meeting of Westinghouse and NRC as items to be for Westinghouse consideration only; however, in the NRC report they are [illegible]ied as "findings".

Verification of the implementation of the actions described above can be accomplished during your next audit of PWRSD. If we can be of any further assistance, or if you have any questions, please contact Mr. E. J. Kreh, (412-256-4584).

Very truly yours,

W. H. Arnold

Attachment

Details Section D.2.b - The following response addresses the specifics of the noted deviation.

D.2.b Implementation of Procedures

Additional information related to this deviation was noted during the review of calculation notes for the zirconium-water reaction error analysis. These calculation notes reported that after modifications had been made to LOCTA IV, recalculated values for the peak clad temperature resulted in a temperature increase of 24°F. It was further noted that no followup action on this item had been performed nor were model changes identified in the resubmitted topical report (WCAP-9220). With respect to this item, paragraph I.b of Section II of 10CFR50, Appendix K, requires that "The description (of the evaluation model) shall be sufficiently detailed and specific to require significant changes in the evaluation model to be specified in amendments of the description. For this purpose, a significant change is a change that result in a calculated fuel cladding temperature different by more than 20°F from the temperature calculated (as a function of time) for a postulated LOCA using the last previously accepted model." DSS/NPR will followup on this item to determine if reporting requirements have been met by Westinghouse.

Response: This particular incident has been dealt with in considerable technical detail with the NRC Staff since the audit. It has been determined that these changes were not "significant" according to 10CFR50, Appendix K, Part II and therefore need not have been reported. However, a letter was sent to the NRC Staff describing the subject changes.

The incident raised a question that perhaps some Westinghouse employees did not fully understand the reporting requirements of 10CFR50, Appendix K, part II. A presentation was made in the first quarter of 1978 to Safeguards Engineering employees on OPR-000-1. As discussed in our first response, Westinghouse will be modifying Nuclear Safety Procedure 5.2. In addition, the new procedure will be reviewed with all affected employees, to stress reporting requirements and responsibilities.

ATTACHMENT B TO PAP-EJH-78-424

Details Section D.1.b. - The following responses address the items provided for consideration:

D.1.b(1): "Procedures do not address how errors identified in computer programs are reported to the USNRC."

Response: See deviation response in the cover letter.

D.1.b(2): "Procedures do not address how warning statements regarding restrictions on code use are resolved."

Response: In carrying out Nuclear Safety Procedure 4.4 (Generation and Updating of Safety Analysis Standards) and Nuclear Safety Procedure 5.4 (Generation of Safeguards Engineering Standards) warning statements regarding recommended restrictions on code applicability are reviewed by cognizant personnel. If the restrictions are determined to be valid, plant safety analyses comply with such restrictions. The results of these reviews are incorporated in Safety Analysis Standards. These standards serve as the guidelines for the analysts and reviewers and are used in their analyses and independent reviews.

D.1.b(3): "Microfische records used in engineering analysis are not always legible."

Response: The microfiche records observed to be not legible were copies of the engineering analysis records. The engineering analysis records used are legible and were available during the audit. This was acknowledged by the audit team.

D.1.b(4): "Documentation did not specify which codes constituted the LOCA/ECCS evaluation model."

Response: The computer codes which were reviewed and approved by the NRC Staff and were locked up in a safe at the Westinghouse NNC for NRC use are the only codes which are part of the model.

Also see our response to D.1.b(7).

D.1.b(5): "The meaning of independent verification is not clearly identified on the Computer Program Change Request Form 55375."

Response: Although we felt that the form in context with the procedure was adequate, Westinghouse agrees that added emphasis through clarification on the form is appropriate. Hence, the form is being changed as follows:

	Old Form	New Form
Middle Section	Executor (Programmer)	Executor (Programmer)
Near Bottom	Executor	Verifier (Other than Programmer)

See Attachment C for a copy of the form with the change indicated.

ATTACHMENT B (cont'd)

D.1.b(6): "Procedures do not require the re-examination and re-evaluation of procedures in the event of code errors."

Response: Westinghouse has not required per se re-examination and re-evaluation of today's procedures after code errors were found because it is our policy to treat any safety related errors in accordance with OPR-600-1 and NS Procedure 1.9 and with subsequent, appropriate actions taken (including re-examination and re-evaluation of procedures if appropriate).

In addition, all procedures are re-reviewed and re-evaluated on a three year cycle according to division policy.

D.1.b(7): "Ancillary codes referred to in computer program documents are not described or referenced adequately."

Response: Westinghouse does not consider ancillary codes which are used to generate input to the evaluation model to be "part of the model."

Ancillary codes are verified and controlled in a manner similar to the NRC reviewe computer codes. The members of the audit team reviewed those procedures during th audit (Safeguards Engineering Standards and Safety Analysis Standards).

D.1.b(8): "Procedures do not address the correction of errors identified in computer program WCAP documents."

Response: Westinghouse does not believe that WCAP typographical errors have caused any computer code error or QA problems - safety related or otherwise. This is because the WCAP is always written after the development and verification is done. Detailed internal standards (Safeguards Engineering Standards and Safety Analysis Standards) are the prime source of information for running computer code and performing an analysis. The WCAP is used only as a background reference.

D.1.b(9): "Safety Analysis Standards do not sufficiently identify code input opt

Response: Although Reactor Protection Analysis has not found this to be a proble to date, this will be considered in the current updating of the Safety Analysis Standards.

D.1.b(10): "Procedures do not address comparisons of new versions of codes agair the same data used to verify the original version."

Response: New versions of a code are compared against old versions of the same code. If the new version gives the same results as the old, it would be unneces to repeat the comparison with data since the comparison would not change. If the new version produced significantly different results, a comparison with original data would be considered as part of the verification procedure.

Verification is done by the developer and it is reviewed by an independent individual or committee. Verification methods are discussed in OPR-300-1:

ATTACHMENT B (cont'd)

A.1 Verification:

The following methods may be employed to verify computer programs other than those recognized to be in the public domain for which no verification need be performed if it can be justified by virtue of its sufficient history of use. This list does not preclude the use of other appropriate methods.

1. Review and check-out of the program logic and listing.

2. Formal review of program objectives, mathematical model and techniques, input and output range(s), etc. by personnel competent in the engineering analysis, design, or safety analysis, and the particular computer programming technology.

3. Comparing the program results with appropriate alternatives, such as one or more of the following:

   a. Sufficient number of hand calculations.
   b. Alternate verified calculational methods.
   c. Results of other verified programs.
   d. Results obtained in experiments and tests.
   e. Known solutions for similar or standard problems.
   f. Measured and documented plant data.
   g. Confirmed published data and correlations.
   h. Results of standard programs and benchmarks.
   i. Parametric sensitivity analysis.

Usually, an independent reviewer performs the first two verification steps above and verifies the developers performance of verification step 3.

D.1.6(11): "Standard No. 19 of the Safety Analysis Standard References an out-of-date version of a computer code."

Response: Safety Analysis Standards are in the process of being updated and Standard No. 19 will be updated.

D.1.b(12): Procedures do not address updating of Safety Analysis Standards.

Response: There is a procedure for revising and distributing Standards for Safeguards Engineering. This procedure was reviewed by NRC during August audit and found to be satisfactory. Similar procedures are being developed by Reactor Protection Analysis.

See Response to NRC comment No. 8 and 11 for additional information.

CONFIGURATION CONTROL COMPUTER PROGRAM CHANGE REQUEST FORM

__ Standard Design Computer Program

Program Name ____________________

____ Other

Permanent File Name ____________________

Description Of Change

Purpose Of Change

Requester ____________________ Manager Approval ____________________

Responsible Engineer Approval ____________________

Cognizant Design Manager Approval ____________________
(Only necessary if Standard Design Code)

Executor (Programmer) ____________________

Charge Number ____________________ Agreed Completion Date ____________________

Completion Date ____________________ Program Revision No. ____________________

Document Number Describing This Change ____________________

Has This Change Altered The Sample Problem Input Deck? ____________________

User Libraries: ____________________

Verification That The Program Has Been Thoroughly Checked On Sample Problems

Verifier (Other Than Programmer)

____________________ Executor Document Number ____________________

Acceptance Date __________ By ____________________ R.

Manager Approval ____________________

Acceptance Date __________ By ____________________ Responsible Engineer

Change Implemented In Production Version On __________ By ____________________
(Control File)

Westinghouse Electric Corporation

Water Reactor Divisions

W H Arnold
General Manager
PWR Systems Division

Nuclear Center
Box 355
Pittsburgh Pennsylvania 15230

December 1, 1978

PA-EJK-78-343

Ref: A) Letter from USNRC (U. Potapovs dated 11/24/78
B) Letter from W (W. H. Arnold), dated 11/3/78

Mr. Uldis Potapovs, Chief
Vendor Inspection Branch
U. S. Nuclear Regulatory Commission
611 Ryan Plaza Drive
Suite 1000
Arlington, Texas 76011

Dear Mr. Potapovs:

Reference A requested additional information to the Westinghouse Audit Response of Reference B. The purpose of this letter is to provide the requested information.

The corrective action taken was to revise Nuclear Safety Procedure 5.2, completed November 29, 1978. This revision was then reviewed and accepted by the USNRC principal inspector during the November inspection.

The action to prevent recurrence is a review of reporting requirements and responsibilities with all affected employees to be completed by January 31, 1979. An initial step in this review was a reissue of the July 15, 1976 letter from Mr. D. F. Ross, Assistant Director for Reactor Safety - Division of Systems Safety - Office of NRR, which dealt with documentation requirements for ECCS models. This letter was distributed to all affected line management on October 6, 1978 for dissemination to the applicable employees.

If we can be of any further assistance, or if you have any questions, please contact Mr. E. J. Kreh at 412-256-4584.

Very truly yours,

W H Arnold

C-E Power Systems
Combustion Engineering, Inc
1000 Prospect Hill Road
Windsor, Connecticut 06095

Tel. 203/688-1911
Telex 99297

POWER SYSTEMS

December 22, 1978

Mr. U. Potapovs, Chief
Licensee Contractor, Vendor
Inspection Branch
United States Nuclear Regulatory Commission
Region IV
Office of Inspection and Enforcement
611 Ryan Plaza Drive, Suite 1000
Arlington, TX 76011

Reference: Docket 99900401/78-04
Letter from U. Potapovs to
M. R. Etheridge received,
December 4, 1978

Dear Mr. Potapovs:

C-E Power Systems Group's response to the deviations described in the referenced report is as follows:

Deviation

Procedures do not exist describing the method by which change to the evaluation model are reported in amendments submitted to the NRC as required by paragraph 1.b of section II of 10CFR50, Appendix K.

Response

A statement addressing the criteria addressed above regarding reportable changes in the ECCS evaluation model will be included in the QADM (Quality Assurance of Design Manual). This corrective action will be completed by April 1, 1979.

The inclusion of the above items in the QADM assure that all interfacing design groups will be cognizant of the requirements regarding changes in the ECCS evaluation model. This preventive action will be completed by April 1, 1979.

Items for consideration by Combustion Engineering, Inc., Management

A letter addressing these items will be issued to the NRC by April 1, 1979.

If you have any questions relative to this response, please contact me.

Very truly yours,

C-E POWER SYSTEMS GROUP

M. R. Etheridge, Vice-President

MRE:ss

Babcock & Wilcox

Power Generation Group

P.O. Box 1260, Lynchburg, Va. 24505

Telephone: (804) 384-5111

October 12, 1978

Mr. U. Potapovs, Chief
Vendor Inspection Branch
U.S. Nuclear Regulatory Commission
Office of Inspection & Enforcement
Region IV
611 Ryan Plaza Drive, Suite 1000
Arlington, Texas 76011

Dear Mr. Potapovs:

Referring to your letter of September 13, 1978, the attached report summarizes B&W responses to NRC Inspection Report No. 99900400/78-03. In addition to describing the steps to be taken to correct the deviation and take preventative action, our reply contains our planned actions in response to the items identified on pages 4-6 of the referenced inspection report.

We have reviewed both the NRC inspection report and our reply, and find that neither includes information that is considered to be proprietary.

Should you have any questions concerning our reply, we will be pleased to discuss them with you.

Very truly yours,

J.H. MacMillan
Vice President
Nuclear Power Generation Division

JHM:jg
Attachment

B&W NPGD (LYNCHBURG) REPLY TO
NRC INSPECTION REPORT NO. 99900400/78-03

RESPONSE TO NOTICE OF DEVIATION

The following is our response to the Notice of Deviation and its three examples:

Notice of Deviation - Example 1

Step 11 of Exhibit B (Certification of Computer Programs) to published procedure NPG-0902-06 (Computer Program Development and Certification) states in part, "...File original documentation in certification files." Further Step 1 defines a typical program package to consist of the request, program, and program manual.

Contrary to the above, the original documentation for the Conditional Certifications for Version 4 of TRAP2 issued January 24, 1978, and Version 4.1 of TRAP2 issued February 9, 1978, were not filed in the Certification Files for the TRAP program.

RESPONSE

The intent of this requirement is for the certification files to contain documented evidence that the programming requests have been reviewed by the Programming Manager and the Applied Mathematics Manager and that the requested programming work has been completed accurately. This requirement for documented evidence can be met with either an original or a copy. NPG-0902-06 will be revised accordingly by December 15, 1978.

Certification files affected by this procedure have been reviewed. Where possible, original documentation has been retrieved from other files and placed in the certification files. Where this has not been possible, the responsible technical staff unit manager has determined that the proper reviews and approvals were obtaine As applicable, evidence of this determination has been placed in the certification files.

Notice of Deviation - Examples 2 and 3

Step 12 of Exhibit B to NPG-0902-06 states in part "...Initiate Program Abstrac and insert in NPGD-TM-338."

Contrary to the above, the Program Abstract for Conditional Certification of Version 3 of TRAP2 issued on December 20, 1977; Version 18 of TRAP issued on March 3, 1978, and Version 4.1 of TRAP2 issued on February 9, 1978, were not inserted in NPGD-TM-338.

Section IV (Program Abstract) of NPG-0902-06 states in part, "...This (Program Abstract) is a computerized format ... that describes certain aspects of the prog (i.e....Responsible Engineer and Progammer, ..."

Contrary to the above, the latest revision (14) to NPGD-TM-338 does not describ (identify) the Responsible Engineer and Progammer.

Notice of Deviation - Examples 2 and 3 (Cont'd)

RESPONSE

The program abstracts were originally developed to provide an accessible document where important information concerning the computer programs could be found. They were to contain the following information: Program Certification Level, Responsible Engineer, Responsible Programmer, Statement of Program Solved and Program Limitations However, the program abstracts contained in NPGD-TM-338 have proved cumbersome to keep current. Further, the information contained in the program abstracts is partially redundant to information in the program manuals.

Methods of providing the above information in a more convenient and controllable form have been evaluated and it has been decided to replace the program abstracts. This will be accomplished as follows:

1. All programs requiring certification will have a program manual containing as a minimum (1) a description of the problem solved; (2) input and output description; and (3) known program limitations.

2. A computerized program listing containing the following information will be developed and maintained:

   a. Computer program name, version number and revision number.

   b. Certification status and date of certification.

   c. Name of programmer and engineer who are currently responsible for maintaining the program.

   d. Current status of the program (i.e., active, obsolete, etc.).

   e. Expiration date for interim and conditional certifications.

The program manuals, coupled with the computerized listing, will provide all of the information presently required to be in the program abstracts.

Necessary procedure changes to reflect this revised system will be made by December 1 1978.

DEVIATION

10CFR50, Appendix B, Criterion V and Section 5 of Topical Report BAW-10096A - Three (3) examples of a failure to follow procedures in the development and revision of safety analysis computer codes. (See Notice of Deviation enclosure).

RESPONSE

An audit of safety analysis computer program certification files will be conducted by NPGD QA prior to January 1, 1979. Any deviations uncovered by this audit will be corrected as outlined in the responses to the specific examples of deviation cited above. In order to prevent recurrence of this deviation, changes to procedures NPG-0902-06 and 0903-03 will be made to strengthen the responsibilities and controls for developing, certifying and changing computer programs. These procedural changes will be implemented by December 15, 1978. Periodic audits will verify compliance with the revised procedures.

REPLY TO NRC INSPECTION REPORT
NO. 99900400/78-03

RESPONSES TO FINDINGS

Our responses and comments to the findings contained in Section C-1-b of the subject inspection report are presented below.

Finding 1

Procedure NPG-0902-06 does not require a specific time limit on how long a computer program can remain in a conditional certification status before it must undergo the full certification process.

Response

NPG-0902-06 will be revised by December 15, 1978 to specify that both conditional and interim certification statements will indicate the allowable time limits for the particular certification status. The conditional certification status will be valid for a period of one year and may be renewed for an additional year upon the approval of the Engineering Department Manager. Interim certification status will have a validity period of three months with no renewal option. In both cases, the conditions necessary for full certification will be specified in the certification documentation.

Finding 2

Procedure NPG-0902-06 does not appear to specify a method for termination of a version of a code which is found to contain an error and/or has been superceded by a new version.

Response

NPG-0902-06 will be revised by December 15, 1978 to require removing the certification for a version of a code in which an error is found, thereby preventing use of the code for safety related calculations until the error is evaluated. Action to be taken when a code version is superceded by a new version will also be defined.

Finding 3

Procedure NPG-0902-06 does not require that users of a code, that subsequently was found to contain an error, be notified of the error and requested to evaluate its effect on past analysis. In addition, the procedure does not require that the corrective actions taken to correct an error found in one version of a code be applied to other versions.

Response

Procedure NPG-0902-02 will be revised to require that unit managers using a code in which an error has been found be notified of the error. Procedures will require that they evaluate the impact of the error on past analyses including those performed with earlier versions of the code. Necessary corrective action will be taken as appropriate. These revisions to NPG-0902-06 will be released by December 15, 1978.

Finding 4

Procedure NPG-0903-03 does not require that the computer program manual be a controlled document similar to the B&W Administrative Manual even though these manuals are used in safety analysis work.

Response

Procedure NPG-0903-03 will be revised by December 15, 1978 to require that distribution of computer program manuals be done in a controlled manner (i.e., controlled distribution list, acknowledgement for receipt of changes, etc.)

Finding 5

Procedure NPG-0902-06 does not specify a method that provides traceability between Form PDS-21177 (Computer Program Certification), Form PDS-21186 (Request for Programming Services), Program, and Program Manual (Revision) submitted for Full and Conditional Certification.

Response

Procedure NPG-0902-06 will be revised by December 15, 1978 to specify a method that provides the necessary traceability of technical requirements/information, review and approval for computer program certification.

Finding 6

Procedure NPG-0902-06 does not specifically define the revision/version notation of the computer program, i.e., is it Version A of TRAP1 or Version 1A of TRAP; Version 2 of TRAP or Version 0 to TRAP2 etc.

Response

Procedure NPG-0902-06 will be revised by December 15, 1978 to specifically define the revision/version notation for computer programs.

Finding 7

Step 8 of Exhibit B to NPG-0902-06 states that the "Technical Staff Engineer" (B&W representatives stated that this meant Technical Staff Manager) "Assign Technical Staff Engineer to evaluate the program." Since a Technical Staff Engineer can initiate the request for certification it is not clear that the same person can perform this evaluation.

Response

The typographical error in the procedure will be corrected. NPG-0902-06 will be clarified by December 15, 1978 to assure an independent review of the computer program. This review will be conducted as part of the computer program certificati process in accordance with the revised procedure.

Finding 8

There appears to be some confusion as to the extent of the applicability of procedure NPG-0402-01 (Processing of NPGD Prepared Calculations) with respect to the independent verification review and documentation of the development, revision, and certification of computer program.

Response

Calculations made during development and independent review of the development, revision and certification of computer programs are processed in accordance with NPG-0902-06 and become part of the certification file. Procedure NPG-0402-01 was not intended to apply to certification calculations and has been revised to to make this clear.

Finding 9

Procedure NPG-0902-06 does not require the documentation of evaluations when detected program errors are determined not to have any safety significance.

Response

Procedure NPG-0902-06 will be revised by December 15, 1978 to require that unit manager, upon detection or notification of a program error, evaluate and document the impact of the error to determine if the error results in a potential safety concern. If the error does not constitute a potential safety concern, documentatio to that effect will be included in the computer program certification file. If a potential safety concern is identified, we will continue to document and process it in accordance with procedure NPG-1707-01.

NRC FORM 335 (7-77)

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER (Assigned by DDC)
NUREG-0653

4. TITLE AND SUBTITLE (Add Volume No., if appropriate)
REPORT ON NUCLEAR INDUSTRY QUALITY ASSURANCE PROCEDURES FOR SAFETY ANALYSIS COMPUTER CODE DEVELOPMENT AND USE

2. (Leave blank)

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S)
BRIAN W. SHERON and ZOLTAN R. ROSZTOCZY

5. DATE REPORT COMPLETED
MONTH JULY | YEAR 1980

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
OFFICE OF NUCLEAR REACTOR REGULATION
UNITED STATES NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C., 20555

DATE REPORT ISSUED
MONTH AUGUST | YEAR 1980

6. (Leave blank)

8. (Leave blank)

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
SAME AS ITEM 9 ABOVE

10. PROJECT/TASK/WORK UNIT NO.

11. CONTRACT NO.

13. TYPE OF REPORT
TECHNICAL REPORT

PERIOD COVERED (Inclusive dates)

15. SUPPLEMENTARY NOTES

14. (Leave blank)

16. ABSTRACT (200 words or less)

As a result of a request from Commissioner V. Gilinsky to investigate in detail the causes of an error discovered in a vendor Emergency Core Cooling System (ECCS) computer code in March, 1978, the staff undertook an extensive investigation of vendor quality control practices as applied to safety analysis computer code development and use. This investigation included conducting inspections of code development and use practices of the four major light water reactor nuclear steam supply system vendors and a major reload fuel supplier.

The conclusion reached by the staff as a result of the investigation is that vendor practices for code development and use are basically sound.

A number of areas were identified, however, where improvements to existing vendor procedures should be made. In addition, the investigation also addressed the quality assurance (QA) review and inspection process for computer codes and identified areas for improvement.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT

19. SECURITY CLASS (This report)
unclassified

21. NO. OF PAGES

20. SECURITY CLASS (This page)
unclassified

22. PRICE
$

NRC FORM 335 (7-77)